普通高校本科计算机专业特色教材精选・网络与通信

计算机网络安全

沈鑫剡　编著

清华大学出版社

普通高校本科计算机专业特色教材精选·网络与通信

计算机网络安全

沈鑫剡　编著

清华大学出版社
北　京

内 容 提 要

这是一本既注重网络安全基础理论，又着眼培养读者解决网络安全问题能力的教材，书中详细讨论了加密算法、报文摘要算法、认证协议等网络安全基础理论，黑客攻击方法和过程，目前主流的网络安全技术，如以太网安全技术、安全路由、信息流管制、VPN、防火墙、入侵防御系统和安全无线局域网等，以及这些防御黑客攻击技术的原理和案例，安全网络的设计方法和过程，安全应用层协议及应用等。

本教材的最大特点是将计算机网络安全理论、目前主流网络安全技术和安全网络的设计过程有机地集成在一起。让读者既能掌握完整、系统的计算机网络安全理论，又具备运用主流网络安全技术实现安全网络的设计能力。

本教材以通俗易懂、循序渐进的方式叙述网络安全知识，并通过大量的例子来加深读者对网络安全知识的理解，内容组织严谨、叙述方法新颖，是一本理想的计算机专业本科生的计算机网络安全教材，也可作为计算机专业研究生的计算机网络安全教材，对从事计算机网络安全工作的工程技术人员，也是一本非常好的参考书。

图书在版编目（CIP）数据

计算机网络安全/沈鑫剡编著. —北京：清华大学出版社，2009.9
（普通高校本科计算机专业特色教材精选・网络与通信）
ISBN 978-7-302-20397-1

Ⅰ. 计…　Ⅱ. 沈…　Ⅲ. 计算机网络—安全技术—高等学校—教材　Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字(2009)第 101089 号

责任编辑：袁勤勇　徐跃进
责任校对：李建庄
责任印制：杨　艳

出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：北京密云胶印厂
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185×260　　**印　张**：19　　**字　　数**：451 千字
版　　次：2009 年 9 月第 1 版　　**印　　次**：2009 年 9 月第 1 次印刷
印　　数：1～3000
定　　价：26.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：010-62770177 转 3103　　产品编号：

出版说明

INTRODUCTION

在我国高等教育逐步实现大众化后，越来越多的高等学校将会面向国民经济发展的第一线，为行业、企业培养各级各类高级应用型专门人才。为此，教育部已经启动了“高等学校教学质量和教学改革工程”，强调要以信息技术为手段，深化教学改革和人才培养模式改革。如何根据社会的实际需要，根据各行各业的具体人才需求，培养具有显著特色的人才，是我们共同面临的重大问题。具体地说，培养具有一定专业特色的和特定能力强的计算机专业应用型人才则是计算机教育要解决的问题。

为了适应21世纪人才培养的需要，培养具有特色的计算机人才，急需一批适合各种人才培养特点的计算机专业教材。目前，一些高校在计算机专业教学和教材改革方面已经做了大量工作，许多教师在计算机专业教学和科研方面已经积累了许多宝贵经验。将他们的教研成果转化为教材的形式，向全国其他学校推广，对于深化我国高等学校的教学改革是一件十分有意义的事情。

清华大学出版社在大量调查研究的基础上，决定组织编写一套“普通高校本科计算机专业特色教材精选”。本套教材是针对当前高等教育改革的新形势，以社会对人才的需求为导向，主要以培养应用型计算机人才为目标，立足课程改革和教材创新，广泛吸纳全国各地的高等院校计算机优秀教师参与编写，从中精选出版确实反映计算机专业教学方向的特色教材，供普通高等院校计算机专业学生使用。

本套教材具有以下特点：

1. 编写目的明确

本套教材是在深入研究各地各学校办学特色的基础上，面向普通高校的计算机专业学生编写的。学生通过本套教材，主要学习计算机科学与技术专业的基本理论和基本知识，接受利用计算机解决实际问题的基本训练，培养研究和开发计算机系统，特别是应用系统的基本能力。

2. 理论知识与实践训练相结合

根据计算学科的三个学科形态及其关系，本套教材力求突出学科的理论与实践紧密结合的特征，结合实例讲解理论，使理论来源于实践，又进一步指导实践。学生通过实践深化对理论的理解，更重要的是使学生学会理论方法的实际运用。在编写教材时突出实用性，并做到通俗易懂，易教易学，使学生不仅知其然，知其所以然，还要会其如何然。

3. 注意培养学生的动手能力

每种教材都增加了能力训练部分的内容，学生通过学习和练习，能比较熟练地应用计算机知识解决实际问题。既注重培养学生分析问题的能力，也注重培养学生解决问题的能力，以适应新经济时代对人才的需要，满足就业要求。

4. 注重教材的立体化配套

大多数教材都将陆续配套教师用课件、习题及其解答提示，学生上机实验指导等辅助教学资源，有些教材还提供能用于网上下载的文件，以方便教学。

由于各地区各学校的培养目标、教学要求和办学特色均有所不同，所以对特色教学的理解也不尽一致，我们恳切希望大家在使用教材的过程中，及时地给我们提出批评和改进意见，以便我们做好教材的修订改版工作，使其日趋完善。

我们相信经过大家的共同努力，这套教材一定能成为特色鲜明、质量上乘的优秀教材。同时，我们也希望通过本套教材的编写出版，为“高等学校教学质量和教学改革工程”作出贡献。

清华大学出版社

前 言

PREFACE

目前计算机网络安全教材是百花齐放，各有特色，但总体上可以分成三类，第一类着重讨论加密、认证算法及其他安全协议，这一类教材的特点是比较详细地讲述网络安全理论，尤其对各种算法和协议做了深入讨论，但缺乏和当前主流安全技术的结合，很难让读者学以致用。第二类主要讨论黑客攻击手段和防御技巧，这一类教材不介绍系统、完整的网络安全理论，有点像黑客攻防大全。第三类把操作系统安全机制、应用程序安全机制和网络安全机制放在一起讨论，当然，所有内容都是浅尝辄止。这三类教材虽然侧重点不同，但有着同样的问题，一是不对当前主流网络安全技术进行深入讨论，二是不在具体网络环境下讨论安全网络的设计方法和过程，对许多问题只是空对空地介绍一些基本概念和方法，没有具体结合目前面临的网络安全问题。因此，难以培养读者解决网络安全问题的实际能力。

对于一本真正以实现将读者领进计算机网络安全知识殿堂为教学目标的教材，一是必须提供完整、系统的网络安全理论，这样才能让读者理解网络安全技术的实现机制，具有进一步研究网络安全技术的能力。二是必须深入讨论当前主流网络安全技术，同时，结合网络安全理论讨论这些安全技术的实现原理，让读者知其所以然，也让读者具备用主流网络安全技术解决实际网络安全问题的能力。三是需要在具体网络环境下讨论运用网络安全技术设计安全网络的方法和过程，给读者提供解决实际网络安全问题的方法和思路，解决读者学以致用的问题。

作为计算机网络安全教材，应该着重讨论和网络有关的安全问题，与操作系统及应用程序有关的安全问题应该在《操作系统》和《算法与程序设计》课程中予以解决，因为离散地讨论一些安全问题会降低该教材的系统性和连贯性，同时，不和整个操作系统结构和程序设计环境结合来讨论操作系统和应用程序安全问题的解决机制，也不利于读者理解、掌握。计算机网络安全教材不可避免地会涉及黑客攻击和防御，但必须从网络总体结构出发，讨论防御黑客攻击的技术，而不是逐个列出攻击手段和防

御方法，将教材变成黑客攻防大全，背离了教材着重于基本理论、基本技术和基本方法的宗旨。

本教材的特色在于:一是为读者提供完整、系统的网络安全理论;二是详细讨论当前主流网络安全技术，并结合网络安全理论讨论这些安全技术的实现原理;三是在实际网络环境下给出运用当前主流安全技术设计安全网络的方法和过程;四是通过构建防御黑客攻击的网络安全体系，讨论运用网络安全技术全方位防御黑客攻击的方法;五是通过门户网站这样的技术给出了精确控制网络资源访问过程的方法。

全书内容安排如下:第1章概论，着重讨论了目前存在的安全问题、解决安全问题的基本方法和构建网络安全体系的必要性。第2章黑客攻击机制，详细讨论了黑客攻击类型、主要攻击步骤及运用网络安全技术防御黑客攻击的基本思路。第3章网络安全基础，详细讨论了加密算法、报文摘要算法、认证协议、IP Sec等网络安全基础理论。第4章安全网络技术，详细讨论了几种广泛应用的网络安全技术及这些网络安全技术防御黑客攻击的机制。第5章无线局域网安全技术，详细讨论了WEP安全机制及存在的安全缺陷，802.11i安全机制解决无线局域网通信安全的原理。第6章虚拟专用网络，详细讨论了第2层和第3层隧道实现数据跨公共分组网络安全传输的方法和过程。第7章防火墙，详细讨论了无状态分组过滤器、有状态分组过滤器及堡垒主机对网络资源访问过程实施严格控制的机制。统一访问控制动态配置网络资源访问控制策略的机制。第8章入侵防御系统，详细讨论了主机入侵防御系统和网络入侵防御系统防御黑客攻击的机制。第9章网络管理和监测，详细讨论了网络管理系统的安全问题和解决方法，监测网络安全状态的机制。第10章安全网络设计实例，详细讨论了运用主流网络安全技术、防火墙、入侵防御系统、网络综合监测系统设计一个实现预定安全目标的安全网络的过程。第11章应用层安全协议，详细讨论了Web安全机制、电子邮件安全传输协议和门户网站精致控制网络资源访问过程的机制。

在教材编写过程中，解放军理工大学工程兵工程学院计算机应用教研室的俞海英、伍红兵、胡勇强、魏涛和龙瑞对教材内容提出了许多很好的建议和意见，其他同事也给予了很多帮助和鼓励，在此向他们表示衷心的感谢。作为一本无论在内容组织、叙述方法还是教学目标都和传统计算机网络安全教材有一定区别的新教材，错误和不足之处在所难免，殷切希望使用该教材的老师和学生批评指正，也殷切希望读者能够就教材内容和叙述方式提出宝贵建议和意见，以便进一步完善教材内容。作者E-mail地址为:shenxinshan@163.com。

作　者

2009年7月

目录

CONTENTS

第 1 章 概 述

CHAPTER

进入信息社会，信息已经成为一种非常重要的资源，它的安全与否已经影响到个人、企业，甚至国家的根本利益。在信息技术领域，信息是一种用二进制表示的数据，它通过信息采集系统存储到计算机中，由计算机进行处理，通过网络在计算机间相互传输。信息安全要求信息在采集、存储、处理和传输过程中不被破坏、窃取和篡改。但信息流动过程中的每一个环节都存在安全问题，存在计算机中的信息有可能被人盗用，侵入计算机的病毒可能破坏整个系统，经过网络传输的信息可能被窃取或篡改，因此，信息安全由计算机安全和网络安全组成，计算机安全负责信息存储和处理过程中的安全事务，主要防止病毒和非法访问。网络安全负责信息传输过程中的安全事务，主要防止用户非法接入，窃取或篡改传输过程中的信息。承担计算机安全功能的实体主要是操作系统和应用程序，当然还有一些用于保护计算机信息资源的实用程序，因此，计算机安全问题通常是操作系统和应用程序的安全问题，目前，大量黑客攻击都是针对操作系统和应用程序的漏洞进行的。但随着互联网的普及和发展，计算机之间为了共享信息资源，用网络互联，这种情况下，网络已经成为病毒的主要传播途径，黑客也常常通过网络远距离窃取存储在某个计算机中的信息，如此，网络安全除了保障信息安全传输外，还须包括阻断病毒传播和黑客非法访问的途径的功能。因此，网络安全在信息安全中占有极其重要的地位，它不仅包含保障信息安全传输的功能，而且还具有识别病毒和正常信息，识别正常访问和黑客攻击，识别授权用户和非授权用户，分类信息资源并对不同信息资源设置相应访问控制策略等功能。但网络安全不承担操作系统和应用程序应该有的安全功能，因此，完整的信息安全系统应该由安全的操作系统、安全的应用程序和安全的网络组成。

1.1 信息安全和网络安全

1.1.1 信息处理时的安全问题

计算机是信息的终端设备，承担着信息采集、处理和存储的功能，信息

处理时的安全问题实际上就是计算机安全问题,目前,计算机最大的安全问题就是病毒、非法访问和拒绝服务攻击。

1. 病毒

病毒是一种具有自复制能力并会对系统造成巨大破坏的恶意代码,它首先隐藏在某个实用程序中,隐藏过程可以由实用程序设计者完成,或者通过病毒感染该实用程序的过程完成。当某个计算机下载该实用程序并运行它时,将运行隐藏在其中的恶意代码,即病毒,病毒将感染其他文件,尤其是可执行文件,并接管一些系统常驻软件,如鼠标中断处理程序。如果病毒接管了鼠标中断处理程序,当鼠标操作激发该中断处理程序时,将首先激发病毒程序,病毒程序可以再次感染其他文件,并视情况执行破坏操作,如清除所有硬盘中的文件。当感染了病毒的实用程序被其他计算机复制并执行时,病毒将蔓延到该计算机。

对于单台计算机,病毒传播主要通过相互复制实用程序完成,对于接入网络的计算机,从服务器下载软件、下载主页、接收电子邮件等操作都有可能感染病毒。接入网络的计算机一旦感染病毒,安全将不复存在,存储在计算机中的信息将随时有可能被破坏,机密信息将随时外泄,非授权用户随时有可能通过远程桌面这样的工具对计算机进行非法访问。

2. 非法访问

非法访问是指非授权用户通过远程登录或远程桌面等工具访问计算机的资源,造成非法访问的原因有病毒、操作系统和应用程序漏洞等。特洛伊木马病毒可以将通过网络接收到的命令作为特权用户输入的命令发送给命令解释程序,从而达到访问系统资源的目的。操作系统和应用程序漏洞可以使普通用户获得特权用户的访问权限,从而使非授权用户访问到本不该访问的资源。

3. 拒绝服务攻击

一种类型的拒绝服务攻击利用操作系统或应用程序的漏洞使系统崩溃,从而使系统无法继续提供有效服务,如缓冲器溢出就是利用应用程序不对需要处理的数据长度进行检测的漏洞,导致应用程序的缓冲器溢出,因而影响系统的正常运行,甚至崩溃,从而使系统无法继续提供有效服务。

另一种类型的拒绝服务攻击是消耗掉某个计算机的有效资源,使其没有用于对正常用户提供有效服务所需要的资源。如攻击者向某个计算机发送大量 IP 分组,以此消耗掉计算机的接入带宽,导致正常用户请求服务的 IP 分组无法到达该计算机,因而无法获得服务。还有 SYN 泛洪攻击,通过用大量无效的 TCP 连接建立请求消耗掉计算机的 TCP 会话表资源,从而使计算机没有用于和正常用户建立 TCP 连接的 TCP 会话表资源。

4. 计算机安全问题的应对措施

一部分计算机安全问题是由操作系统或应用程序的漏洞引起的,解决这些安全问题的方法是及时为漏洞打上补丁,因此,必须有一套保障所有终端系统都能及时通过补丁软件消除已发现漏洞的机制,最大限度地避免系统遭到攻击。及时发现操作系统和应用程序的漏洞,并通过下载补丁软件予以修补并不是网络安全的范畴,但目前,由于网络中系统众多,各个系统的管理、应用人员的计算机水平又都参差不齐,要求所有系统的管理人

员都能及时发现系统所安装的操作系统和应用程序的漏洞，并通过下载补丁软件予以修补是比较困难的，因此，需要在网络中安装监测系统，由网络监测系统对所有系统安装的操作系统和应用程序进行监测，获取它们的类型和版本号，检测它们是否修补了已发现的漏洞，并对有安全问题的系统进行提醒。安装网络监测系统是一种通过网络安全机制来解决网络中所有系统因为操作系统和应用程序的漏洞而引发的安全问题的方法。

一部分计算机安全问题是需要网络安全机制予以解决的，如拒绝服务攻击，需要网络中的监测设备能够及时检测出这种异常信息流，并对其流量予以管制。网络安全机制也可以识别出含有病毒的信息流，并阻断其网络传播途径。

1.1.2　信息传输时的安全问题

目前，信息通过网络进行传输，信息传输时的安全问题毋庸置疑是网络安全问题，它涉及非法接入、信息窃取、源地址欺骗和拒绝服务攻击等，这些安全问题基本上由网络安全机制解决。

1. 非法接入

每个企业都有内部网络，或许这样的内部网络也和 Internet 相连，但只允许企业内部人员访问企业内部网络的资源。所谓非法接入是指非企业内部人员连接到了企业内部网络并获得访问内部网络资源的途径。攻击者实现非法接入的手段很多，如通过笔记本计算机直接接入企业内部网络的某个以太网交换机端口，通过远程拨号接入方法接入企业内部网络，利用无线局域网接入企业内部网络等。

2. 信息窃取

如果攻击者非法接入企业内部网络，或者信息需要经过公共传输网络进行传输，传输的信息很容易被拦截、窃取和篡改。如攻击者通过修改路由器路由表，将信息发送给攻击者的终端。攻击者通过类似集线器这样的共享式传输设备连接到内部网络的某条主干传输通路上等。这样，经过网络传输的信息有可能被攻击者截获，攻击者可以窃取这些信息，甚至篡改后继续转发给原始目的终端。

3. 源地址欺骗

源 IP 地址是信息发送者的一个重要标识符，接收者常用 IP 分组的源 IP 地址来确定信息发送者的身份。为了控制信息流动，也常对允许交换信息的子网进行限制，因此，IP 分组的源和目的 IP 地址也是确定信息是否允许经过路由器转发的依据。攻击者为了达到非法访问的目的，或是为了躲避责任，常用本不存在的，或是其他合法用户的 IP 地址，作为自己发送的 IP 分组的源 IP 地址。

4. 拒绝服务攻击

网络中路由器的缓冲器和路由表空间，结点之间链路的带宽都是用于保证信息正常传输的资源，拒绝服务攻击通过消耗掉这些资源，使网络无法正常传输信息，导致传输过程中的信息被阻塞，甚至丢弃。如攻击者通过发送包含大量无用路由项的路由消息给路由器，使路由器的路由表溢出，导致路由器无法正常转发 IP 分组。如大量被攻击者控制的终端同时向某个子网发送大量信息，导致通往该子网的路径因为阻塞而无法正常转发有用信息。

5. 传输安全问题的应对措施

防护攻击者非法接入的方法是构建一个能够阻断非法接入途径的内部网络，如以太网的接入认证机制、安全端口机制、无线局域网的安全机制等。防止信息窃取、篡改的最好办法是加密和报文摘要技术。防止源地址欺骗的方法是除了源 IP 地址，还采用数字签名来标识信息发送者，同时，通过测试接收 IP 分组的端口是否连接通往源 IP 地址所确定的发送者的路径来判别 IP 分组源 IP 地址的真伪。防止拒绝服务攻击的机制有信息流管制、有效信息鉴别及过滤等机制。

1.1.3 电子交易时的安全问题

随着电子商务的开展和普及，各种电子交易平台出现在网络中，人们开始通过网络实现购物、交易和缴费等活动。这种情况下，电子交易的安全性直接决定电子商务的发展和普及。电子交易的安全性涉及计算机安全和信息传输安全，但除了计算机安全和信息传输安全外，还存在其他安全问题，如通过伪造的某个银行网站，骗取登录用户的银行卡卡号和密码，从而实现非法目的的案例，这就要求提供一种能够对双方身份的真实性进行鉴别的机制。另外，攻击者可能在某次正常电子交易时截获用户请求购物的消息，虽然，加密和报文摘要技术使攻击者无法窃取和篡改该消息，但攻击者经过一段时间后，再次重发该消息，导致购物网站以为该用户将再一次进行购物，造成用户的损失，这就要求提供能够鉴别重复请求消息的机制，解决这些安全问题也是网络安全的范畴。

1.2 信息安全目标

信息安全目标是实现信息的适用性、保密性、完整性、不可抵赖性和可控制性等。

1.2.1 适用性

适用性是信息被授权实体访问并按需使用的特性。通俗地讲，就是做到有权使用信息的人任何时候都能使用已经被授权使用的信息，信息系统无论在何种情况下都要保障这种服务；而无权使用信息的人，任何时候都不能访问到没有被授权使用的信息。

实现信息适用性的安全目标要求保障计算机系统的适用性和网络系统的适用性，计算机系统不因病毒和拒绝服务攻击而崩溃。网络系统不因拒绝服务攻击而发生阻塞、路由器崩溃。电子交易过程中能够正确鉴别交易双方的身份，并对交易请求进行重复性检测。

1.2.2 保密性

保密性是防止信息泄露给非授权个人或实体，只为授权用户使用的特性。通俗地讲，信息只能让有权看到的人看到，无权看到信息的人，无论在何时，用何种手段都无法看到信息。

实现信息保密性的安全目标要求计算机系统能够严格控制信息访问过程，防止非授权用户的非法访问。网络系统能够严格控制非授权用户接入网络，按照安全等级划分子

网，并对子网间的信息交换过程进行控制。同时，网络通过监测信息流能够发现远程用户通过感染特洛伊木马病毒的计算机系统进行非法访问的过程。另外，存储在计算机系统中的信息和经过网络传输的信息必须加密，这样，即使信息被非法访问或在传输过程中被非法用户截获，攻击者也无法获得有用信息。

1.2.3 完整性

完整性是信息未经授权不能改变的特性。通俗地讲，信息在计算机存储和网络传输过程中，非授权用户无论何时，用何种手段都不能删除、篡改、伪造信息。

实现信息完整性的安全目标主要依靠报文摘要算法，通过对信息附加完整性检验值(Integrity Check Value，ICV)或消息完整性编码(Message Integrity Code，MIC)，能够鉴别出信息在存储或传输过程中是否被篡改。

1.2.4 不可抵赖性

不可抵赖性是信息交互过程中，所有参与者不能否认曾经完成的操作或承诺的特性，这种特性体现在两个方面，一是参与者开始参与信息交互时，必须对其真实性进行鉴别；二是信息交互过程中必须能够保留下使其无法否认曾经完成的操作或许下的承诺的证据。

实现信息不可抵赖性的安全目标主要依靠认证机制和数字签名技术，认证机制能够对信息交互双方进行身份鉴别，确定其身份的真实性。数字签名技术能够对信息的有效性作出承诺，并且能够验证这种有效性承诺。

1.2.5 可控制性

可控制性是对信息的传播及内容具有控制能力的特性。通俗地讲，就是可以控制用户的信息流向，对信息内容进行审查，对出现的安全问题提供调查和追踪手段。

实现信息可控制性的安全目标要求网络系统能够根据不同的安全等级和应用划分子网，并对子网间传输的信息流进行控制和过滤，能够检测出有害信息并加以干预。

1.3 网络安全机制

网络安全是信息安全的重要组成部分，担负着实现信息安全目标所要求的大部分责任，目前用于实现网络安全的机制主要有加密、报文摘要算法和数字签名技术，接入控制技术和认证机制，分组检测和信息流管制机制，入侵防御机制，应用层安全机制等。

1.3.1 加密、报文摘要算法和数字签名技术

1. 加密

如图1.1所示，加密是指用加密算法(E)和密钥(K_1)对明文(P)进行运算，使其成为无法正常识别的密文(Y)的过程，而解密是加密的反过程，是指用解密算法(D)和密钥(K_2)对密文(Y)进行运算，重新得到明文(P)的过程。

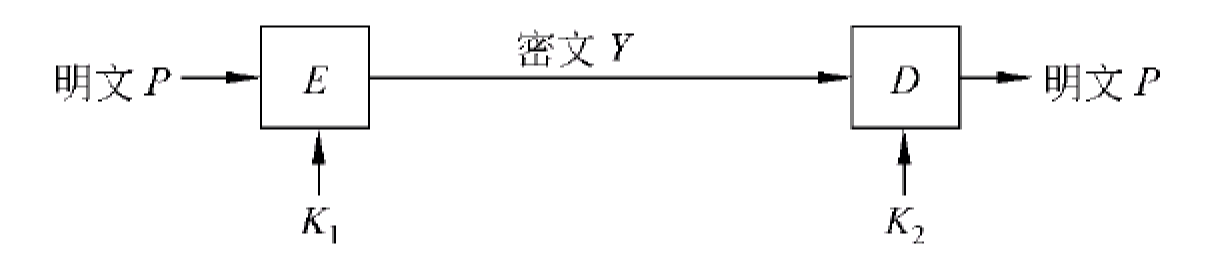


图 1.1 加密解密过程

$$Y = E_{K_1}(P) \tag{1.1}$$

$$P = D_{K_2}(Y) \tag{1.2}$$

$$D_{K_2}(E_{K_1}(P)) = P \tag{1.3}$$

式(1.1)是加密公式,式(1.2)是解密公式,式(1.3)是还原明文过程。

密文的安全性取决于解密算法和密钥 K_2,但在 Internet 中,为了规范通信双方的安全通信机制,往往采用标准的加密解密算法。这种情况下,密钥 K_2 的安全性决定安全通信机制的成败。密钥 K_2 的安全性不仅仅指密钥是否容易泄露,还有密钥是否能够被猜测到,是否能够通过明文和对应的密文分析出密钥,而这一点又和加密解密算法有着密切的关系。加密解密过程是安全通信机制的基础,是保证信息保密性的最有效方法。

2. 报文摘要

信息完整性检测需要确定信息在传输过程中是否被损坏和篡改,解决这一问题的简单方法是发送端将传输的信息复制为相同的两份,并对复制后的信息加密。接收端对接收到的信息解密,并对两份信息进行比较。如果相同,表示信息在传输过程中未被损坏;否则,表示信息在传输过程中已被篡改。为了检测信息完整性,重复传输信息,而且需要对重复的信息进行加密,这极大地增加了终端的处理负担和网络的传输负担。现实生活中,常常用摘要来概括文章的主要内容,而摘要的字数比文章原文少得多,同理,用于报文完整性鉴别的报文摘要(Message Digest,MD)也必须具有如下特性:

- 给定报文 P,能够很容易地计算出报文摘要 MD(P),且报文摘要 MD(P)的二进制位数比报文 P 少得多;
- 知道报文摘要 MD(P),不能反推出报文 P;
- 从计算可行性讲,对于任何报文 P,无法找出另一个报文 P',$P \neq P'$,但 MD(P)=MD(P');
- 即使只改变报文 P 中一位二进制位,也使得重新计算后的 MD(P)变化很大。

这样,当需要对传输的信息进行完整性鉴别时,发送端将对根据明文计算出的报文摘要进行加密,并将加密后的报文摘要附在明文后一起发送给接收端。接收端接收到明文和附在明文后面的加密后的报文摘要后,先对加密后的报文摘要解密,还原出发送端计算出的报文摘要,然后对明文进行报文摘要运算,并将计算结果和解密后的报文摘要进行比较,如果相等,表示信息在传输过程中未被篡改,如果不相等,则表示信息已经被篡改,整个过程如图 1.2 所示。

3. 数字签名

数字签名要求发送者在发送的信息中留下无法抵赖的痕迹,如果发送的信息用加密算法 E 和密钥 K_1 经过加密运算,且能够证明:

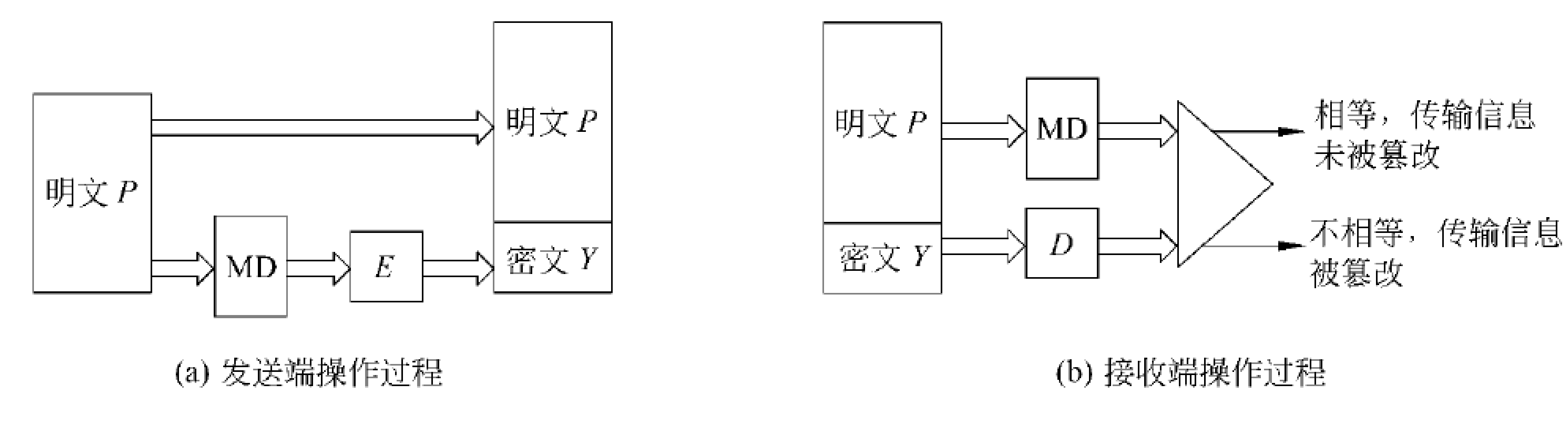


图 1.2　用报文摘要技术鉴别信息完整性的过程

(1) 只有发送者拥有密钥 K_1；

(2) 密钥 K_2 和密钥 K_1 一一对应，对应密钥 K_1 和加密算法 E，只能用密钥 K_2 和解密算法 D 才能解密。

那么，只要证明报文用加密算法 E 和密钥 K_1 进行了运算，发送者就无法否认发送过该报文的事实，而证明报文用加密算法 E 和密钥 K_1 进行了运算的过程就是用解密算法 D 和密钥 K_2 对报文进行解密运算的过程，如图 1.3 所示。

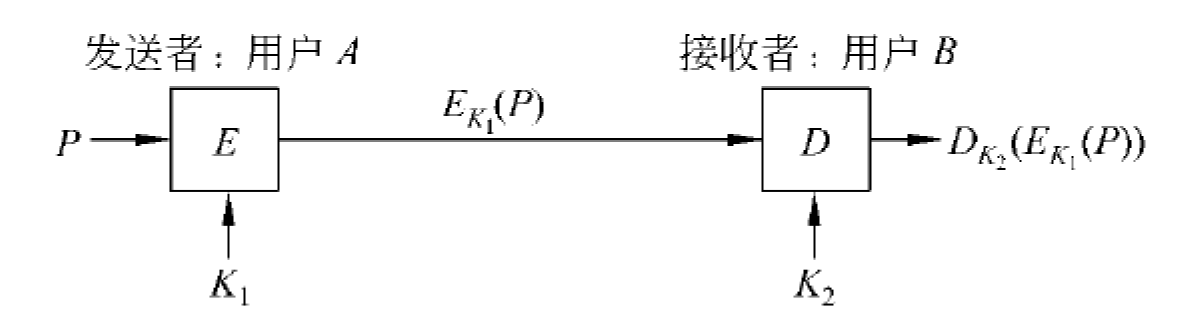


图 1.3　数字签名过程

根据目前的计算能力，某个用户用数字签名技术对另一个用户进行栽赃的可能性是不存在的，任何用户无法事先伪造一个密文 Y，然后用另一个用户对应的解密密钥 K_2 对伪造的密文 Y 进行解密运算，得到预期的、不利于另一个用户的明文 P。但任何信息用某个用户对应的解密密钥 K_2 进行解密运算后都有结果，虽然这种结果毫无意义，但从原理讲，这种结果都可认定是该用户发送的明文。为了防止这种无聊的操作产生不良的后果，应该对数字签名的认定过程加一些限制。另外，由于加密操作是计算密集型操作，需要占用较多的处理时间，如果仅仅为了证实报文的数字签名而对整个明文 P 进行加密运算，所付出的计算成本也太大，因此，需要对数字签名的证实过程进行改进。改进后的数字签名证实过程如图 1.4 所示，用户 A 用加密密钥 K_1 对明文 P 经过报文摘要运算后得到的报文摘要 MD(P)进行加密运算，产生数字签名(E_{K_1}(MD(P))，将明文 P 和数字签

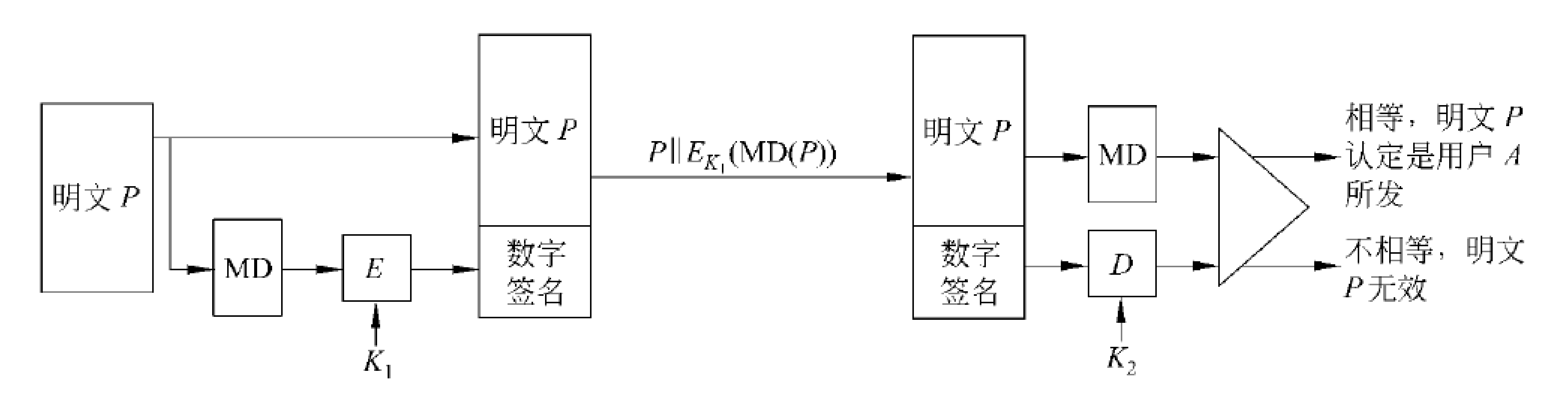


图 1.4　改进后的数字签名证实过程

名一同发送给用户 B。用户 B 认定明文 P 是用户 A 发送的前提是：用用户 A 对应的解密密钥 K_2 对数字签名进行解密运算后得到的结果与对明文 P 进行报文摘要运算后得到的结果相同，即 D_{K_2}（数字签名）$=$MD(P)。图 1.4 所示的数字签名证实过程，既避免对整个明文 P 进行加密运算，又通过数字签名和明文 P、发送者密钥 K_1 之间的关联将明文 P 和发送者绑定在一起。

1.3.2 接入控制和认证机制

接入控制主要指对终端接入传输网络的过程实施控制，只允许授权用户的终端接入传输网络，并通过传输网络访问网络中的信息资源。它必须完成两方面功能，一是对用户身份进行认证，二是保证访问网络资源的用户确实是已通过身份认证的用户。认证机制就用于实现这两个功能，它一方面对接入用户的身份进行确认，另一方面为得到确认的用户约定一个唯一的用户标识符，以后该用户用于访问网络资源的信息中必须包含该标识符，以便传输网络鉴别。

简单的用户身份认证过程如图 1.5 所示，用户接入传输网络前，先向认证者注册，由认证者对注册后的用户分配用户名和口令，同时在认证者的注册数据库中记录下用户的注册信息和分配的用户名和口令。当某个用户接入传输网络时，首先向认证者发送用户名和口令，认证者在注册数据库中检索接入用户发送的用户名和口令，如果检索到相同的用户名和口令对，表示接入用户是授权用户，允许他通过传输网络访问网络中的信息资源，否则，予以拒绝。接入用户以明文方式向认证者传输用户名和口令是不可取的，因为，经过传输网络传输的任何信息都有可能被截获，因此，必须通过一种安全的方式向认证者传输用户名和口令。图 1.6 中，接入用户先向认证者发送用户名，认证者如果在注册数据库中检索到该用户名，就用随机数生成器产生一个随机数，并将该随机数发送给接入用户，接入用户将该随机数和自己的口令串接(图 1.6 中用 ‖ 表示串接操作符)在一起，如果随机数为 123456，口令为 ABCDEF，则串接操作后的结果为 123456ABCDEF，然后对串接操作后的结果进行报文摘要运算，并将运算结果发送给认证者，认证者根据保持的随机数和注册数据库中的口令进行同样的运算，并将运算结果和接入用户发送的运算结果进行比较，如果相等，表示是授权用户；否则，予以拒绝。

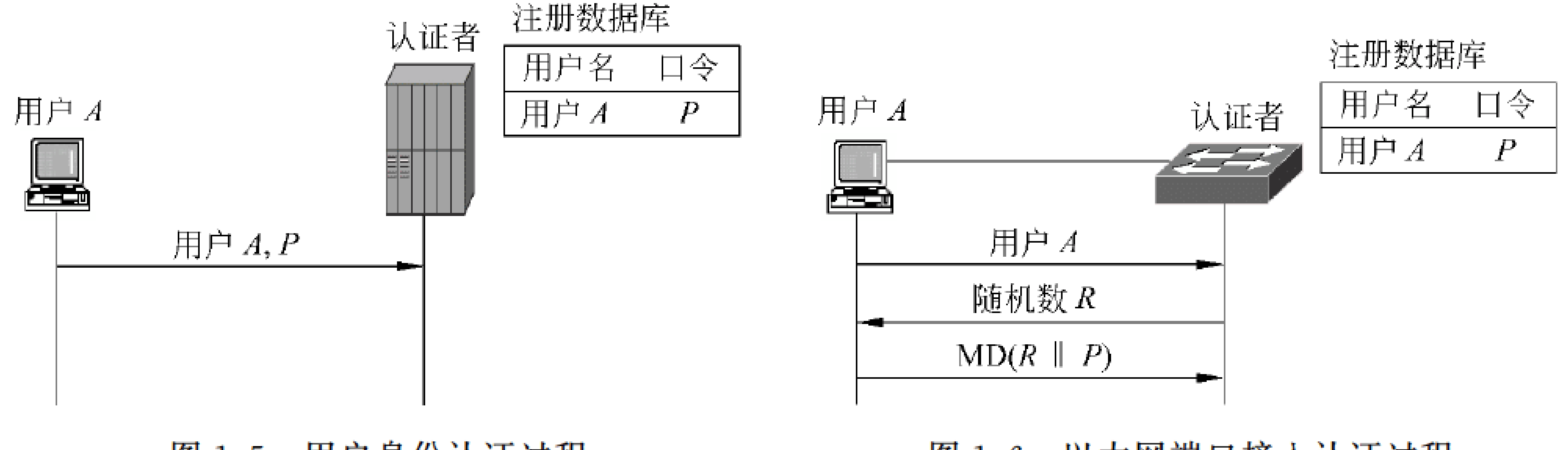


图 1.5 用户身份认证过程　　图 1.6 以太网端口接入认证过程

认证机制不仅需要完成接入用户的身份认证，还需约定用于鉴别信息流是否由该授权用户发送的机制，不同情况下，采用不同的鉴别机制。在图 1.6 中，如果用户终端直接

接入以太网交换机端口，而且由连接用户终端的以太网交换机作为认证者对接入用户进行身份认证，以太网交换机连接用户终端的端口在完成对用户终端的身份认证前只能接收、发送和认证有关的控制报文，不能转发普通数据报文。只有完成认证后，才允许转发普通数据报文，而且，一旦该端口重新进行了物理连接，端口必须重新开始对接入用户的认证过程。这样，可以保证通过该端口转发的数据都是授权用户发送、接收的数据，这就是以太网接入交换机基于端口的认证机制的工作原理。

直接在接入交换机完成对接入用户的身份认证是比较直观的方法，但对移动用户有些不便，可能需要在多个接入交换机配置某个移动用户的注册信息。另外，一般的网络安全策略允许接入用户自由访问一些公开的网络资源，但对一些敏感的网络资源实施控制，因此，对于图 1.7 所示的网络结构，只需要在以太网交换机 S_4 的端口 1 对需要通过该端口访问网络中敏感信息资源的用户进行身份认证，但必须和接入用户约定一种用于鉴别信息流是否是授权用户发送的机制。在以太网中，比较简单的办法是一旦通过对某个接入用户的身份认证，就在端口的接入控制表中记录下该用户终端的 MAC 地址，以后，只有在端口对应的接入控制表中能够检索到源 MAC 地址的 MAC 帧才能通过该端口予以转发，其他 MAC 帧一律丢弃。

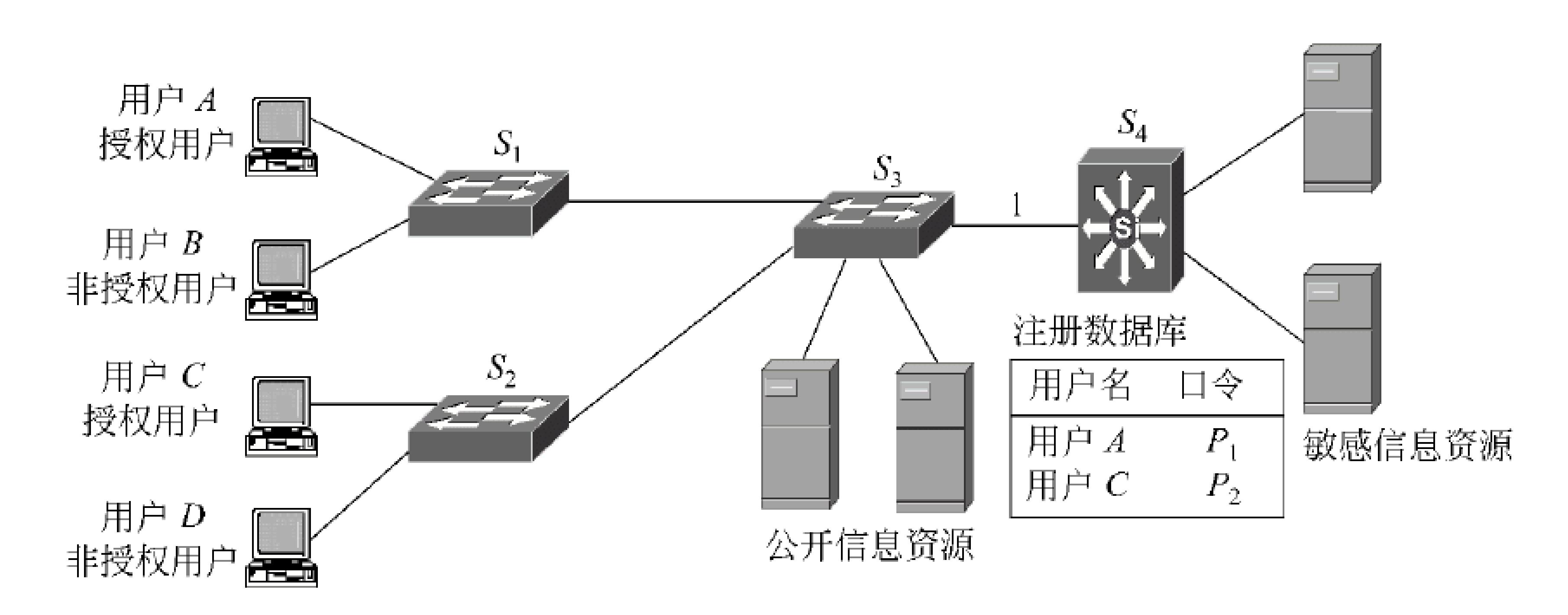


图 1.7 大型以太网接入用户认证机制

由于非授权用户可能在以太网中截获授权用户发送的 MAC 帧，并因此通过伪造授权用户的 MAC 地址冒充授权用户访问敏感信息资源。尤其对于无线局域网，同一基本服务集(Basic Service Sets，BSS)中的终端均可接收到其他终端发送的或接入点(Access Point，AP)设备转发的 MAC 帧，因此，非授权用户冒充授权用户更加容易。鉴于以上情况，单纯用源 MAC 地址作为鉴别信息流是否是授权用户发送的依据是不安全的。为了解决这一问题，通常由认证者和授权用户约定一个只有他们双方知道的密钥 K，授权用户发送的 MAC 帧中的数据都用密钥 K 进行加密，认证者接收到这样的 MAC 帧后，用源 MAC 地址检索出对应的密钥 K，并用密钥 K 对 MAC 帧中的数据进行解密，这样，只有源 MAC 地址和某个授权用户关联的 MAC 地址相同，且可用和该授权用户关联的密钥解密 MAC 帧中数据的 MAC 帧才被确定为该授权用户发送的 MAC 帧，并予以转发。当然，用密钥对数据进行加密和解密运算是非常消耗 CPU 处理能力的事情，会降低认证者转发数据的能力，因此，需要在转发性能和访问安全之间取舍。

对用户终端接入以太网或无线局域网这样的传输网络的过程进行控制称为接入控制，当某个用户访问某个服务器时，同样需要对用户访问服务器的过程进行控制，这种控制称为访问控制，它们的基本原理是相同的，但访问控制更多用双方约定的密钥作为鉴别访问请求是否是授权用户发送的依据。

1.3.3 分组检测和信息流管制机制

1. 分组检测

分组检测机制用于控制信息在各个子网间的流动，如图 1.8 所示。一个企业网通常由三个区组成：信任区、非军事区和非信任区。信任区是企业内部网，只允许企业内部人员对其进行访问；非军事区（Demilitarized Zone，DMZ）主要由企业对外公开的服务器群组成，如 Web 服务器、电子邮件服务器等；非信任区主要指外部网络，如 Internet。一般的访问控制策略是：企业内部人员允许访问非军事区中的服务器，还可以对 Web 服务器进行管理，如修改主页等。从使用方便性出发，企业内部人员应该允许任意访问外部网络，但为了保证内部网络的安全，同时也避免类似 P2P 这样的应用大肆占用网络带宽的情况发生，对企业内部人员访问外部网络也进行限制。外部网络只允许访问非军事区中的服务器，不允许访问企业内部网络中的资源，分组检测机制就用于实现这样的访问控制策略。

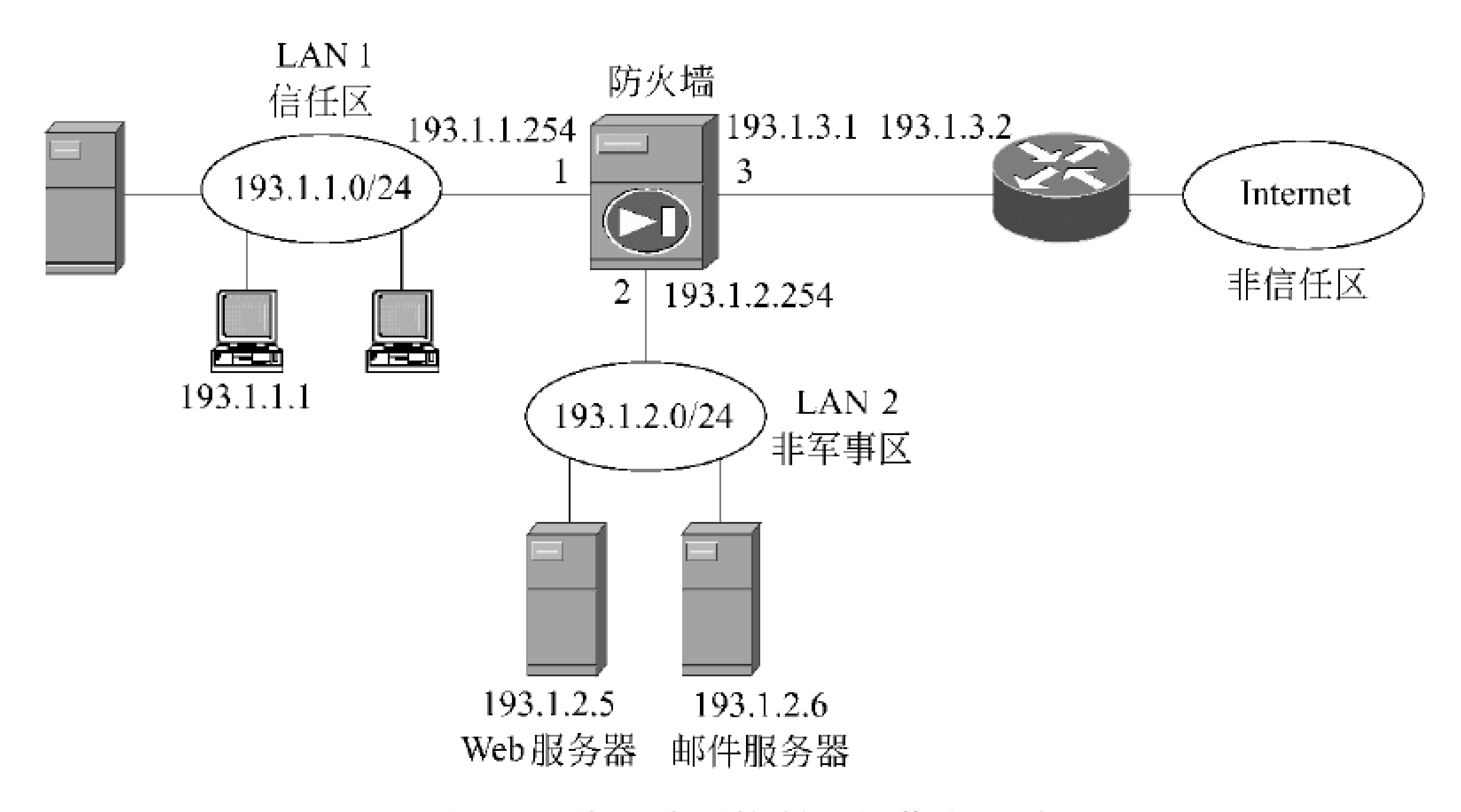


图 1.8 分组检测控制区间信息流动

图 1.8 中的防火墙是实现分组检测的主体，它首先将各个区和端口绑定在一起，如图 1.8中防火墙的端口 1、2 和 3 分别绑定信任区、非军事区和非信任区。然后定义访问控制策略：允许信任区中终端访问非军事区中的 Web 服务器。防火墙分组检测机制保证区间只有符合访问控制策略的信息流动。

图 1.9 给出了访问控制策略规定的区间信息流动过程，它意味着整个访问过程的第一个报文必须是从防火墙端口 1 接收到，并从端口 2 发送出去的 SYN=1、ACK=0 的建立 TCP 连接请求报文，在完成该报文转发前，任何其他报文都因为不符合访问控制策略而被丢弃。而符合访问控制策略的第二个报文只能是从防火墙端口 2 接收到，并从端

口1发送出去的SYN＝1、ACK＝1的建立TCP连接响应报文。符合访问控制策略的后续TCP报文如图1.9所示，任何时候当且仅当符合访问控制策略的TCP报文才能经过防火墙传输，这就保证了区间只允许流动和访问控制策略定义的访问过程相关的信息。

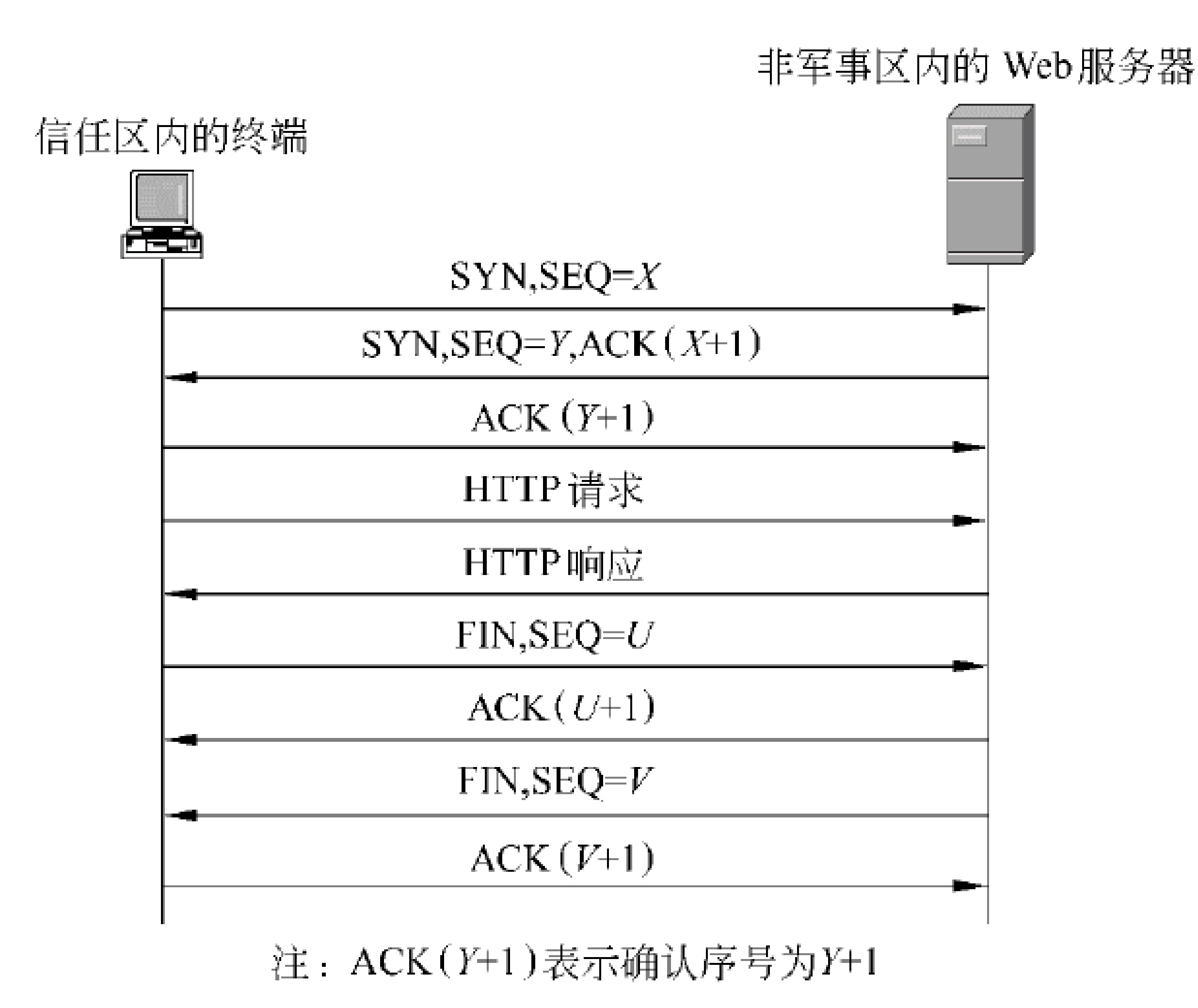


图1.9 访问控制策略规定的区间信息流动过程

2. 信息流管制

分组过滤能够对区间流动的信息实施控制，但无法限制信息流量，许多攻击都是利用合法的访问过程展开的，如拒绝服务攻击——SYN泛洪，就是利用允许非信任区中终端访问非军事区中服务器的访问控制策略对非军事区中的Web服务器实施攻击的，因此，需要在防火墙连接非信任区的端口对来自非信任区的信息的流量实施管制。另外，ISP对接入用户的带宽也有所限制，信息流管制通过对不同类型的信息流设定带宽阈值，保证该类信息的流量在设定阈值之下。

1.3.4 入侵防御机制

入侵防御系统与防火墙功能不同，防火墙的功能主要在于控制各子网间(或各区间)信息传输，尤其是外部网络和内部网络之间的信息传输，但入侵防御系统主要检测内部网络中的信息流模式，尤其是经过关键网段的信息流模式，发现可能对网络造成伤害的异常情况，及时示警，以便网络安全管理员及时作出响应。

入侵防御系统的应用如图1.10所示，一个完整的入侵防御系统由若干探测器和一个管理服务器组成，探测器负责监测经过某个网段的信息流。在发现异常的情况下，一方面向管理服务器报告，另一方面及时对异常信息流实施干预。管理服务器负责安全策略设计，探测器配置，探测器报告的异常情况分析、归类，最终形成有关网络安全状态的报告提供给网络安全管理员。

入侵防御系统发现系统异常的机制有协议异常、攻击特征、后门检测及信息流异常等。协议异常检测是对协议操作过程、报文格式、报文各字段值进行分析，看其是否和协

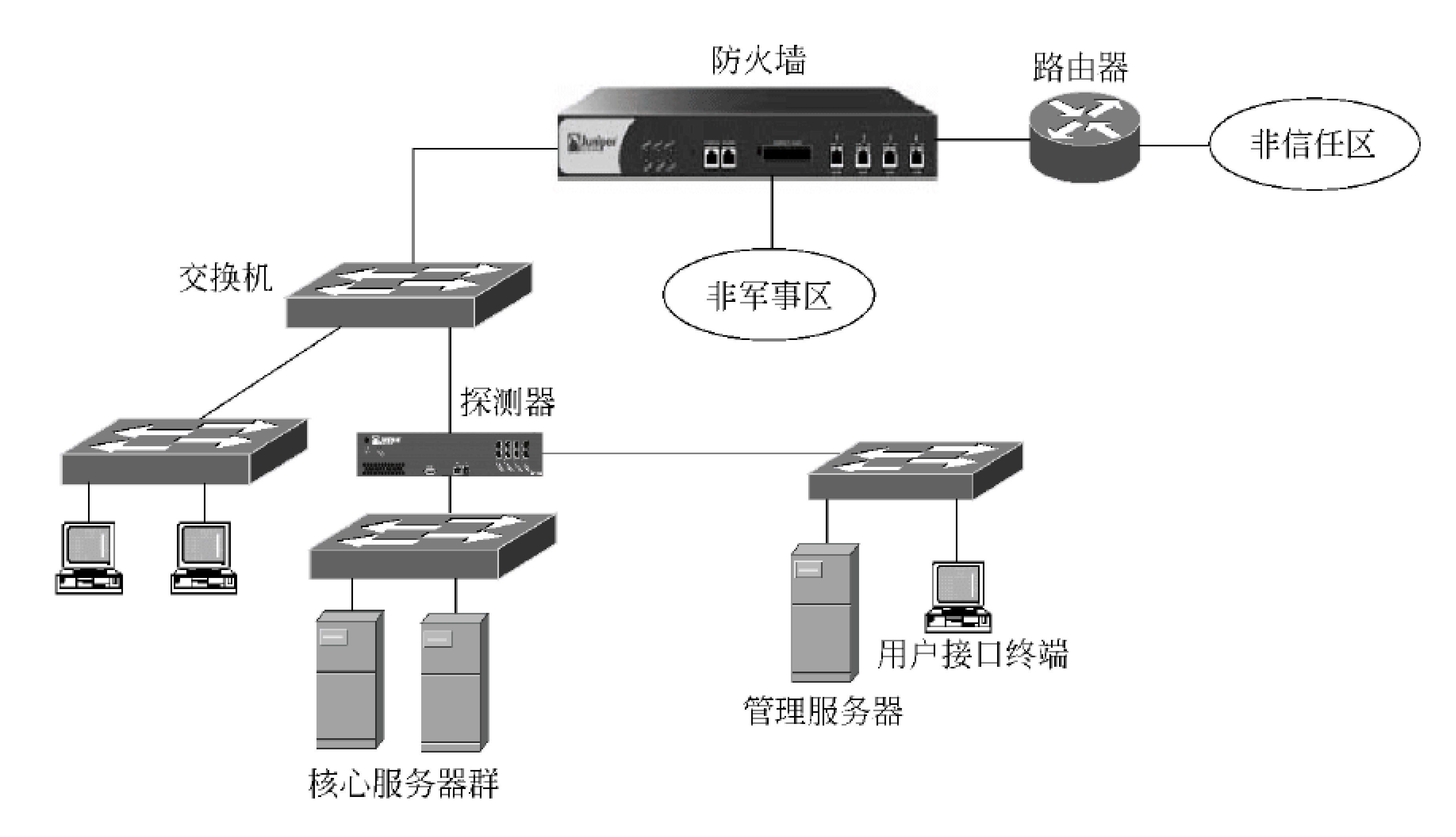


图 1.10 入侵防御系统应用实例

议标准不符。

攻击特征检测和杀病毒软件相似，将已经发现的攻击手段中的特征信息提取出来，构成一个特征信息库，如果信息流模式和攻击特征库中的某个攻击的特征信息相符，表明发现了攻击，通知网络安全管理员采取相应措施。

所谓后门，就是类似特洛伊木马的病毒程序，一旦系统感染这种病毒程序，攻击者可以随时登录系统进行破坏活动。由于攻击者登录系统后进行的一系列操作交互性很强，通过监测交互性很强的信息流模式（报文很短且交换频繁等）来发现某个系统可能存在后门。这种检测机制有可能误将正常的交互性操作当作后门报告给网络安全管理员。

信息流异常是指某种信息流模式的频繁出现程度，已经超过了正常情况下统计到的平均值，可以将这种情况视为攻击，或攻击前奏。比较典型的是端口扫描，攻击者为了找到系统漏洞，用端口扫描方式来发现系统哪些端口是打开的。所谓某个端口是打开的，是指别的终端用该端口号作为目的端口号向该系统发送建立 TCP 连接请求报文时，该系统发出同意建立 TCP 连接的响应报文。由于攻击者事先并不知道系统哪些端口是打开的，采用从小到大，逐次增加端口号的方法不断尝试建立 TCP 连接，因此，这种情况下，短时间内会出现大量具有相同目的 IP 地址，但不同目的端口号的建立 TCP 连接请求报文。假定正常情况下通过统计得到的平均值是每秒针对某个系统发出的建立 TCP 连接请求报文数为 20 个，则可将阈值设定为 40 个/秒，如果一秒内具有相同目的 IP 地址，不同目的端口号的建立 TCP 连接请求报文数超过了 40 个，则可以认为发生了针对某个系统的端口扫描事件，需要向网络安全管理员报告，以便采取对策。

入侵防御的最大困难在于如何平衡安全性和正确性，为了网络安全，应该将异常的条件规定得十分严格，这样可以将大多数攻击检测出来，但也将大量原本正常的信息流模式作为异常情况报告给网络安全管理员，增加了网络安全管理员的负担。如果为了提高发现攻击的正确性，有必要调整异常的条件，可能减少了误报异常的情况，但也有可能漏过

了许多攻击。因此，配置入侵防御系统的安全策略是一件十分困难的事，是需要在较长时间内不断调整的过程。

1.3.5 应用层安全机制

1. Web 服务器认证和数据加密

Web 服务器已经成为进行网络购物、缴费等电子商务的平台，用户需要和 Web 服务器交换一些私密信息，因此，在和某个 Web 服务器进行电子商务活动前，必须认证 Web 服务器的真实性，如通过银行网站进行网络缴费前，必须确认所访问的网站是指定银行网站，而不是不法分子伪造的。另外，由于通过网络传输的信息存在被窃取的可能性，必须对相互传输的私密信息加密，但加密操作的前提是用户和网站约定相同的加密算法和只有用户和网站知道的密钥。由于用户访问网站的随机性，用户和网站之间事先通过协商约定加密算法和密钥的方法不具有可操作性，因此，必须设计一种能够使用户和网站动态约定加密算法和密钥的机制。

2. 电子购物

电子购物涉及用户、商家和银行，用户通过访问商家网站选择商品，商家在向用户提供商品前必须确保能够获得用户支付的货款，因此，需要由银行向商家为用户提供信用担保，并在商家向用户提供商品后，完成用户至商家的资金转账。这一系列操作涉及身份认证、银行账户认证、用户支付能力确认等安全机制。

1.4 网络安全体系

1.4.1 TCP/IP 体系结构

网络是由多层功能组合而成的复杂系统，目前用于表示网络功能层之间关系的网络体系结构是 TCP/IP 体系结构，如图 1.11 所示。

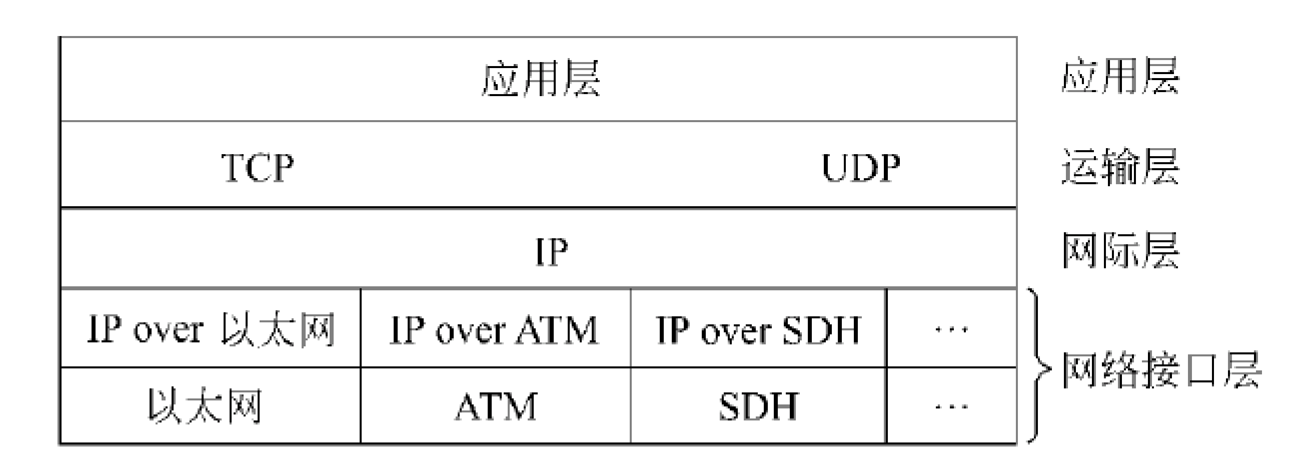


图 1.11 TCP/IP 体系结构

对于图 1.11 所示的复杂的网络体系结构，任何一种技术都无法有效解决网络安全问题，必须在网络的每一层增加安全功能，而且各层安全功能必须相互协调、相互作用，构成一个有机的整体，这样一个由各层安全功能构成的有机整体就是网络安全体系。

1.4.2 网络安全体系结构

网络安全体系结构如图 1.12 所示，它由两部分组成，一部分是网络安全基础，它所包

含的加密、报文摘要算法、数字签名技术及认证和各种安全协议是所有网络安全技术的基础。另一部分是作用于网络每一层的安全技术，它犹如立体盾牌，挡住了攻击者对网络各层功能块的攻击。

<table>
<tr><td colspan="6">HTTPS、SET、门户网站、PGP等</td><td colspan="2">应用层</td></tr>
<tr><td colspan="6">有状态检测等、信息流管制</td><td colspan="2">运输层</td></tr>
<tr><td colspan="6">安全路由协议、IPSec、分组过滤、NAT等</td><td colspan="2">网际层</td></tr>
<tr><td rowspan="2">以太网</td><td>安全端口、接入认证</td><td rowspan="2">无线局域网</td><td>802.11i</td><td rowspan="2">接入网络</td><td>接入认证、VPN L2TP</td><td>链路层</td><td rowspan="2">网络接口层</td></tr>
<tr><td>电缆、光缆保护、电磁屏蔽</td><td>信号能量控制</td><td>电缆、光缆保护、电磁屏蔽</td><td>物理层</td></tr>
<tr><td colspan="6">加密、报文摘要和数字签名技术
TLS、RADIUS等</td><td colspan="2">网络安全基础</td></tr>
</table>

图 1.12 网络安全体系结构

作用于网络接口层的网络安全技术和具体的传输网络有关，如以太网 MAC 层的网络安全技术主要有安全端口和接入认证，这和用户通过双绞线传输媒体接入某个以太网交换机端口以实现网络连接的机制有关。而无线局域网由于没有用户物理接入网络的过程，接入认证不仅成为必须有的功能，而且其安全性要强于以太网的接入认证。传统的接入网络主要解决用户接入 Internet 的问题，它主要包括远程拨号、非对称数字用户线(Asymmetric Digital Subscriber Line，ADSL)和以太网接入技术，并用点对点协议(Point-to-Point Protocol，PPP)、802.1X 或 DHCP＋WEB 技术对接入用户进行身份认证和 IP 地址分配，这些内容已经反映在“计算机网络”课程的教材中。这里讨论的接入技术是一种用户通过公共传输网络，如 Internet，实现远距离接入企业内部网络，并作为企业内部网络的一个用户终端访问企业内部网络中的资源的机制。

读者或许发现，网络接口层所列出的传输网络或是局域网，或是接入技术，没有广域网，如同步数字体系(Synchronous Digital Hierarchy，SDH)和异步传输模式(Asynchronous Transfer Mode，ATM)等。这主要因为局域网和接入技术是用户终端接入网络的最基本途径，而将用户终端接入网络是攻击者攻击网络过程中的第一个步骤，因此，对接入网络的用户终端实施控制，将有效抑制攻击者对网络的攻击。

仅在接入阶段实施控制并不能完全保障网络安全，这一方面是因为攻击者可能非法获得了合法用户的用户名和口令，能够伪造成合法用户接入网络；另一方面，大量攻击并不来自外部，而是来自内部，来自内部感染了病毒的用户终端和怀有敌意的内部员工。这种情况下，必须在内部网络结构中实施安全技术，如根据不同安全等级划分子网，由分组过滤技术对子网间信息交换过程实施控制，这样，连接在较低安全等级的子网上的用户终端将无法访问较高安全等级的子网中的资源，因而无法对这些资源实施攻击。路由器中的路由表是网络最重要的资源之一，因此，必须保证路由表中路由项的正确和完整，这由安全路由协议实现。

有些企业内部网络可能允许内部用户终端访问 Internet 资源，但不允许外部用户访

问企业内部网络中的资源，因此，不能由分组过滤技术简单隔绝内部网络和外部网络之间的信息流动，只允许属于由内部网络中终端发起建立的 TCP 连接的 IP 分组在外部网络和内部网络之间流动，不允许建立由外部网络终端发起的，目标为内部网络中终端的 TCP 连接，这就需要涉及运输层的有状态检测技术。有些情况下，允许外部网络终端访问一些内部网络资源，如内部网络的 Web 服务器，但攻击者常常利用这一机会发动拒绝服务攻击，不仅使外部网络终端无法合理访问内部网络资源，有可能还殃及内部网络终端之间的信息交换过程。由于拒绝服务攻击常常是利用合法访问途径来消耗网络带宽和服务器资源，因此，必须用信息流管制技术对这些超出正常访问所需要流量的信息流实施管制，以免网络和服务器因为过载而丧失服务能力。

Internet 中可以自由设立网站，当然，也会出现通过网站实施违法活动的事情，虽然可以由法纪部门对违法网站进行管制，但网络安全技术也必须提供相应的保障措施，如 HTTPS（HTTP over TLS）就在实施信息交互前对双方身份进行认证。SET 就能保证在电子交易过程中对类似信用卡卡号和密码这样的用户机密信息实施有效保护。

构建一个能够保证网络内的用户不受攻击，机密信息不被窃取，所有网络服务能够正常进行的安全网络，是计算机网络安全的目标，但实现这一目标非常困难，或许针对特定网络应用环境，可以构建一个相对有效的网络安全体系，但无法构建一个适用于所有网络应用环境的网络安全体系，这也是本教材强调在具体网络应用环境下讨论构建网络安全体系的过程的原因。这一方面可以通过构建针对具体网络应用环境的网络安全体系，来加深理解各种网络安全技术的实现机制和适用范围，它们之间的相互作用过程；另一方面只有这样做，才能讲深讲透网络安全理论、网络安全技术和特定网络应用环境下的网络安全体系之间的关系，才能理清网络安全的知识脉络，树立完整的网络安全概念。

习　题

1.1　在实际应用过程中是否碰到安全问题？是单机安全问题还是网络安全问题？试分析引发安全问题的原因及可能对策。

1.2　试分析单机环境下和网络环境下病毒的传播过程，说明网络环境下病毒更容易、更快速传播的原因。

1.3　说明以太网可能遭受的攻击，试给出防御这些攻击的方法。

1.4　无论加密运算，还是解密运算都是改变原始信息内容的运算过程，因此，单独的加密运算或解密运算都能达到改变原始信息内容的目的，试给出几种加密、解密运算，并分析它们的安全性。

1.5　报文摘要算法特性中，哪两点最重要，一旦违背，对报文摘要算法的应用会造成什么样的后果？

1.6　数字签名有效的前提是什么？认证发送者身份和数字签名有什么异同？

1.7　防火墙如何控制信息流的传输过程？

1.8　入侵防御系统和防火墙有什么不同？试给出用入侵防御系统隔断病毒传播路径的例子。

1.9 为什么解决网络安全需要构建网络安全体系？说明应用层安全技术并不能保证用户正常访问 Web 服务器的原因。

1.10 接入网络是实施网络攻击的第一步，有什么机制可以阻止非法终端接入网络？

1.11 一台感染了蠕虫病毒的计算机向某个服务器发送大量垃圾信息，导致服务器丧失正常服务功能，有什么机制可以避免这一情况发生？

1.12 经常有不法分子伪造银行网站套取用户账号和密码，如何防止误登录这样的非法网站？

第2章 黑客攻击机制

CHAPTER

知己知彼，百战不殆，网络安全和黑客攻击是矛盾的两个方面，只有充分了解黑客攻击机制，才能有效构建网络安全体系。黑客攻击手段多种多样，构建网络安全体系也不能头痛医头，脚痛医脚，应该从原理上把握黑客攻击机制并加以抑制，因此，讨论黑客攻击机制不能只是罗列现有的黑客攻击案例，而是着重于黑客攻击的一般原理和基本方法。

2.1 黑客攻击类型

2.1.1 非法访问

非法访问分两种情况：一种是对内部网络资源进行非法访问，另一种是对开放资源进行非法访问。实施前一种非法访问首先要实现非法接入，只有接入内部网络，建立黑客和内部网络资源之间的数据传输通路，才能进行非法访问。后一种非法访问是在存在黑客和开放资源之间数据传输通路的情况下，对开放资源进行越权操作，如修改某个公开网站的网页。

1. 非法接入

如果黑客不是内部人员，图2.1和图2.2是两种常见的非法接入内部网络的方式。许多内部网络允许内部员工通过PSTN远程访问内部网络资源，图2.1是实现内部员工通过拨号接入方式接入内部网络的网络结构。内部网络通常为需要通过拨号接入方式接入内部网络的员工配置用户名和口令，内部员工通过PPP建立访问内部网络资源的数据传输通路时，远程用户接入设备需要验证接入用户的用户名和口令，只有注册用户才能建立访问内部网络资源的数据传输通路。但通过收集有关拥有该内部网络的企业的信息，不难猜测到有效的用户名和口令，如查询到企业某个售后技术支持者的姓名，该姓名的全拼音和数字123456很有可能就是有效用户名和口令。

为了方便内部员工访问内部网络资源，通常在会议室和其他空旷的地方安装无线局域网，虽然802.11i已经提高了无线局域网的安全性，但为了

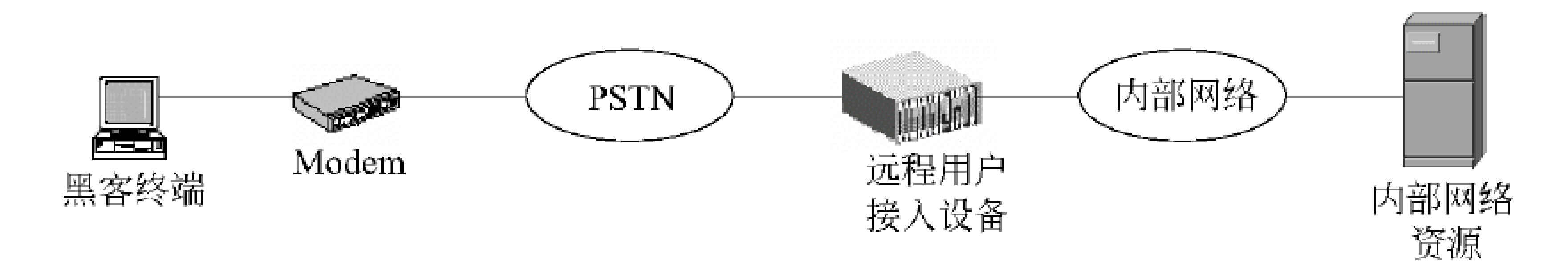


图 2.1 以拨号接入方式接入内部网络

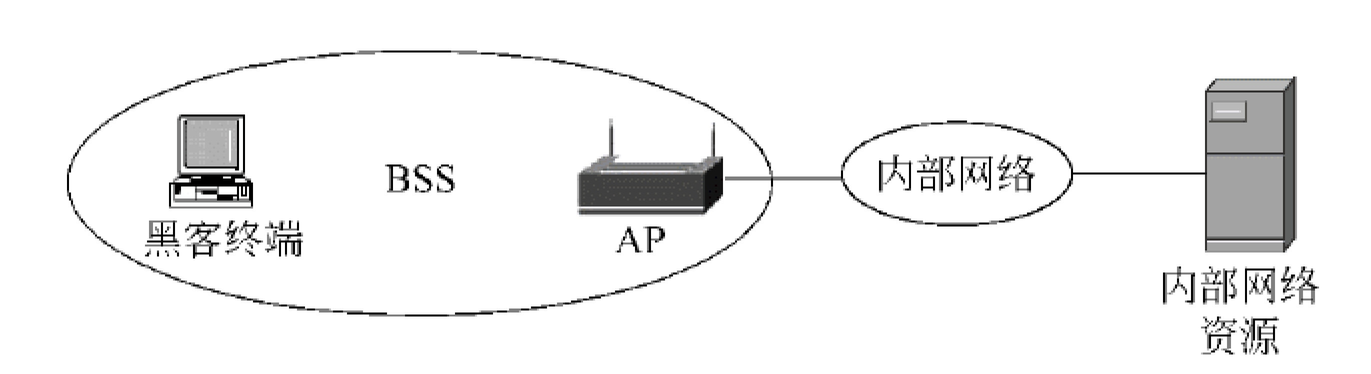


图 2.2 通过无线局域网接入内部网络

和大量采用等同有线安全(Wired Equivalent Privacy,WEP)技术的用户兼容,接入点(Access Point,AP)往往被配置成用 WEP 安全技术进行身份认证和信息加密,而黑客非法接入一个采用 WEP 安全技术的无线局域网是非常容易的事情,何况有的无线局域网甚至没有采用任何安全技术进行接入用户的身份认证和信息加密操作。

2. 非法访问网络资源

在建立黑客和内部网络资源之间的数据传输通路后,黑客可以开始对内部网络资源的非法访问。假定内部网络资源是一台安装 Windows 系统的主机,实施非法访问就是越权修改、删除 Windows 系统中的文件。

远程攻击一台 Windows 系统主机的途径大致分为两种:一是针对 Windows 独有的组网协议和服务,主要包括服务器消息块(Server Message Block,SMB)、微软远程过程调用(Microsoft Remote Procedure Call,MSRPC)和 NetBIOS 协议以及基于 NetBIOS 协议的 NetBIOS 会话服务(NetBIOS Session Service)和 NetBIOS 名字解析服务(NetBIOS Names Service,NBNS),这些服务允许人们通过通用 API 对一台安装 Windows 系统的主机进行远程特权访问;二是针对各种在 Windows 系统上实现的 Internet 服务,如 HTTP、SMTP、POP3 和 NNTP 等。

下面简要讨论黑客通过这两种远程攻击途径非法访问内部网络资源的过程。如果 Windows 系统开放了 SMB 服务,黑客可以尝试连接一个共享卷,比如 IPC $ 或 C $ 共享卷。但连接某个共享卷需要口令,一种方式是猜测口令,就像刚才所说的,猜测到一个有效口令并不是想象中的那样难。另一种方式是截取授权用户和 Windows 系统之间传输的信息,然后离线进行破译,获得访问共享卷所需要的口令。连接共享卷后,可以对共享卷中的文件进行操作,删除或修改共享卷中的文件。

通过在 Windows 系统上实现的 Internet 服务对 Windows 系统实施远程攻击的主要途径,是利用 Internet 信息服务(Internet Information Service,IIS)中的缺陷,通过攻击 IIS 的侦听端口,使 IIS 缓冲区溢出,因而执行攻击程序。攻击程序把一个以 SYSTEM 权限运行的远程命令 shell 发送到黑客终端上的任意端口,这样,黑客可以通过该远程 shell 对 Windows 系统进行控制。

非法访问所涉及的操作系统和应用程序的安全问题不是本教材讨论的范畴，因此，不对操作系统和应用程序的缺陷及因此造成的后果展开详细讨论，但网络安全体系要尽可能减少，甚至消除因为操作系统和应用程序的缺陷而造成的不良后果。

2.1.2　窃取和中继攻击

窃取是指黑客非法获得用户之间正常传输的信息，中继攻击（亦称重放攻击）是指黑客非法获得用户甲传输给用户乙的信息后，延迟一段时间，然后再一次转发给用户乙的攻击手段。在电子商务中，这种攻击手段可能造成严重后果，假定用户甲要求用户乙提供2000 件某类商品的订单被黑客窃取，但仍然到达用户乙，并因此完成了这次交易。当黑客延迟一段时间后再一次将窃取的订单转发给用户乙时，使用户乙误认为用户甲又下了提供 2000 件某类商品的订单，引发用户乙和用户甲之间的商务纠纷。

1. 用集线器窃取信息

用集线器窃取信息的过程如图 2.3 所示，由于集线器是共享设备，从集线器某个端口输入的信息将从集线器所有其他端口发送出去，因此，如果某个黑客终端通过集线器连接到某个主干网段上，黑客将窃取流经该网段的全部信息。通过集线器只能窃取信息，不能截获信息，信息仍将传输到目的终端。

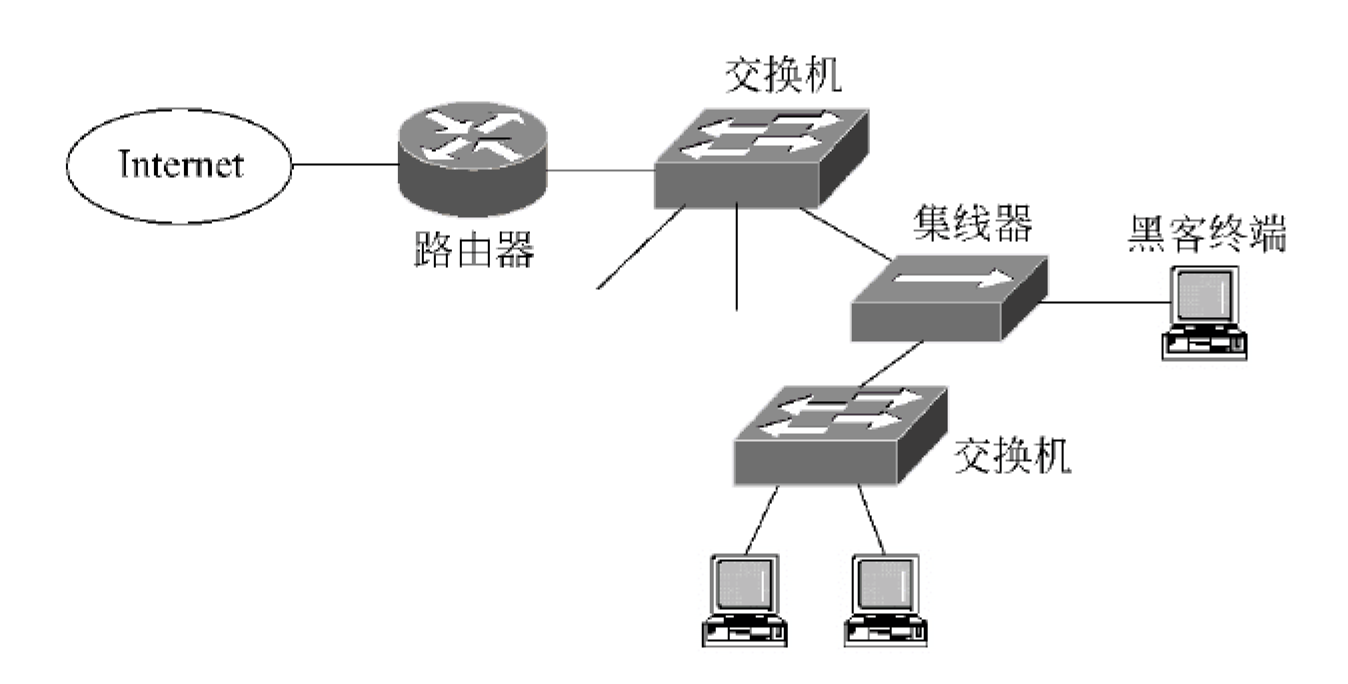


图 2.3　用集线器窃取信息的过程

2. ARP 欺骗

图 2.4 所示的网络结构中，黑客终端分配的 IP 地址为 IP *C*，网卡的 MAC 地址为 MAC *C*，而终端 *A* 分配的 IP 地址为 IP *A*，网卡的 MAC 地址为 MAC *A*，正常情况下，路由器 ARP 缓冲区中应该将 IP *A* 和 MAC *A* 绑定在一起，当路由器需要转发目的 IP 地址为 IP *A* 的 IP 分组时，或者通过 ARP 解析出 IP *A* 对应的 MAC 地址（ARP 缓冲区中没有 IP *A* 对应的 MAC 地址），或者直接从 ARP 缓冲区中检索出 IP *A* 对应的 MAC 地址 MAC *A*，将 IP 分组封装在以 MAC *R* 为源 MAC 地址，MAC *A* 为目的 MAC 地址的 MAC 帧中，然后，通过连接路由器和终端 *A* 的以太网将该 MAC 帧传输给终端 *A*。当黑客终端希望通过 ARP 欺骗来截获发送给终端 *A* 的 IP 分组时，它首先广播一个 ARP 请求帧，请求帧中将终端 *A* 的 IP 地址 IP *A* 和自己的 MAC 地址 MAC *C* 绑定在一起，路由器接收到该 ARP 请求后，在 ARP 缓冲区中将 IP *A* 和 MAC *C* 绑定在一起，当路由器需要转发目的 IP 地址为 IP *A* 的 IP 分组时，将该 IP 分组封装在以 MAC *R* 为源 MAC 地

址，MAC C 为目的 MAC 地址的 MAC 帧中，这样，连接路由器和终端的以太网将该 MAC 帧传输给黑客终端，而不是终端 A，黑客终端成功拦截了原本发送给终端 A 的 IP 分组。为了更稳妥地拦截发送给终端 A 的 IP 分组，黑客终端通常在实施拦截前，通过攻击瘫痪掉终端 A。

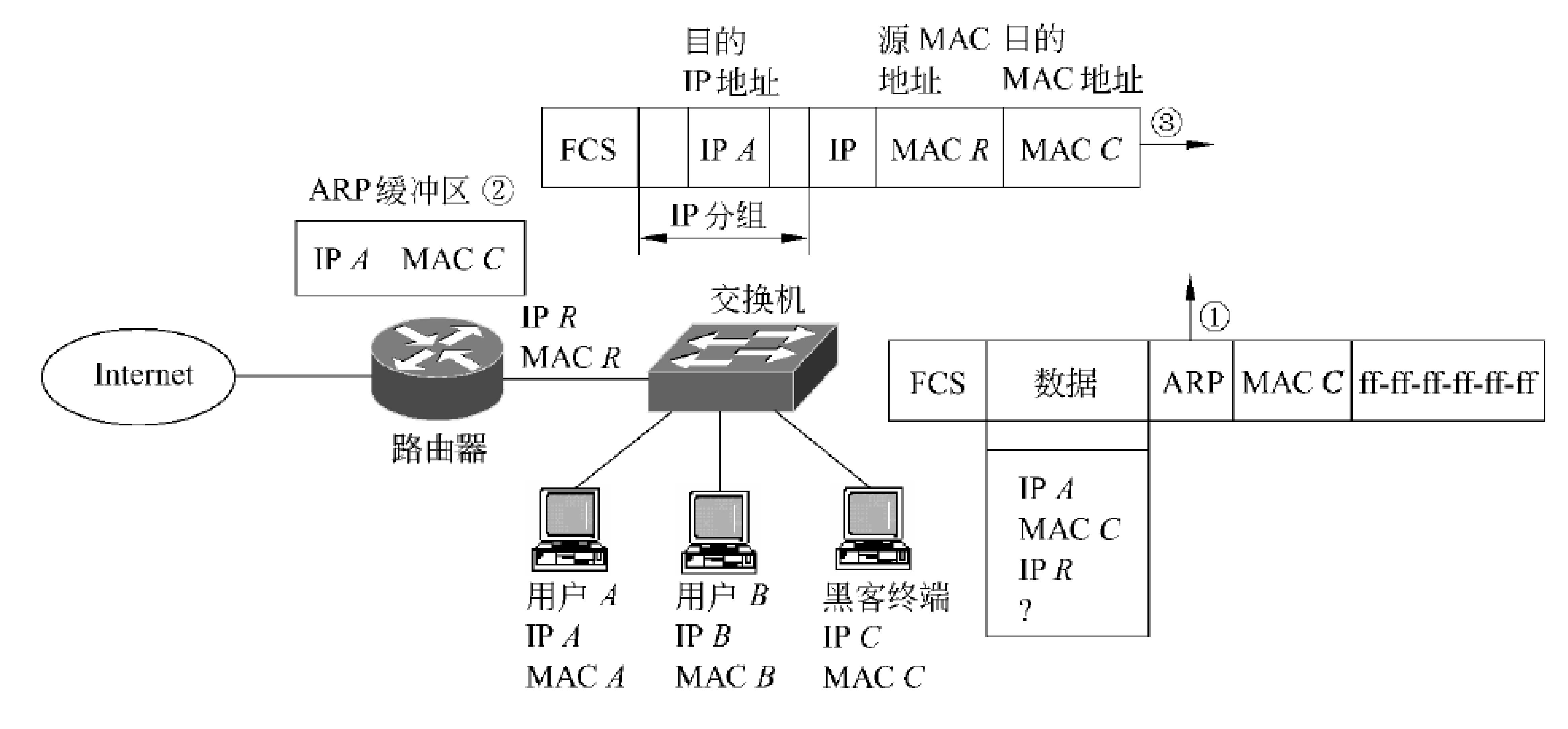


图 2.4 ARP 欺骗过程

3. 伪造路由信息

针对图 2.5 所示的网络拓扑结构，路由器 R_1 通过路由协议生成的正确路由表如图 2.5中路由器 R_1 正确路由表所示，这种情况下，终端 A 发送给终端 B 的 IP 分组，将沿着终端 A→路由器 R_1→路由器 R_2→路由器 R_3→终端 B 的传输路径到达终端 B。如果某个黑客终端想截获连接在 LAN 1 上终端发送给连接在 LAN 4 上终端的 IP 分组，通过接入 LAN 2 中的黑客终端发送一个以黑客终端 IP 地址为源地址、组播地址 224.0.0.9 为目的地址的路由消息，该路由消息伪造了一条黑客终端直接和 LAN 4 连接的路由项，路

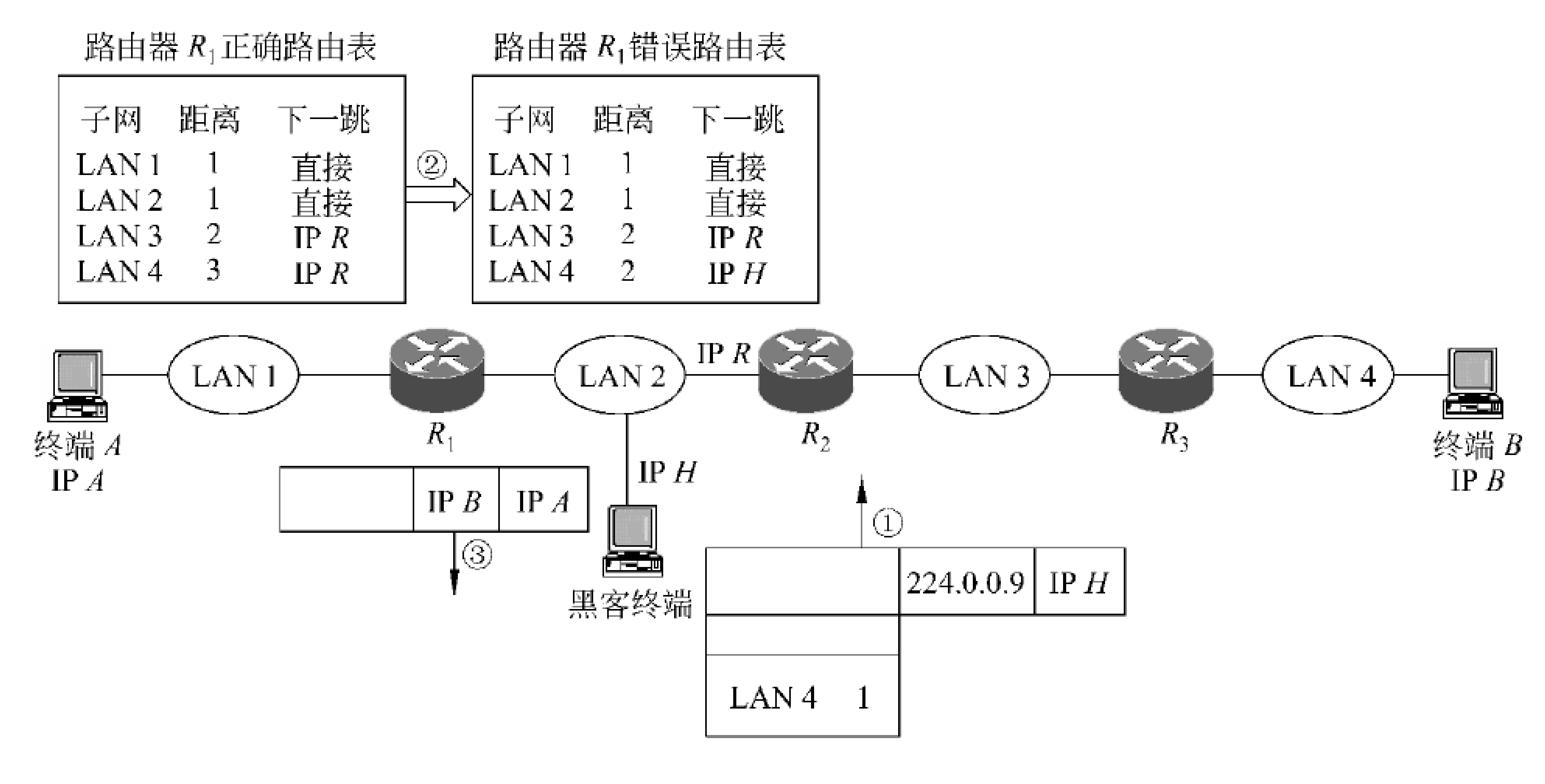


图 2.5 伪造路由过程

由器 R_1 和 R_2 均接收到该路由消息，对于路由器 R_1 而言，由于伪造路由项给出的到达 LAN 4的距离最短，将通往 LAN 4 传输路径的下一跳路由器改为黑客终端，如图 2.5 中路由器 R_1 错误路由表所示，并导致路由器 R_1 将所有连接在 LAN 1 上终端发送给连接在 LAN 4 上终端的 IP 分组错误转发给黑客终端。图 2.5 中终端 A 发送给终端 B 的 IP 分组，经过路由器 R_1 用错误的路由表转发后，不是转发给正确传输路径上的下一跳路由器 R_2，而是直接转发给黑客终端。

2.1.3 拒绝服务

拒绝服务(Denial Of Service，DOS)攻击就是用某种方法耗尽网络设备或服务器资源，使其不能正常提供服务的一种攻击手段。SYN 泛洪攻击是一种通过耗尽服务器资源，使服务器不能正常提供服务的攻击手段；Smurf 攻击是一种通过耗尽网络带宽，使被攻击终端不能和其他终端正常通信的攻击手段。

1. SYN 泛洪攻击

如图 2.6 所示，黑客终端伪造多个本不存在的 IP 地址，请求和 Web 服务器建立 TCP 连接，服务器在接收到 SYN＝1 的建立 TCP 连接请求后，为请求建立的 TCP 连接分配资源，并发送 SYN＝1、ACK＝1 的确认响应。但由于黑客终端是用伪造的 IP 地址发起的 TCP 连接建立过程，服务器发送的确认响应不可能到达真正的网络终端，因此，也无法接收到来自客户端的确认报文，该 TCP 连接处于未完成状态，分配的资源被闲置。当这种未完成的 TCP 连接耗尽服务器的资源时，就无法对正常的建立 TCP 连接请求作出响应，Web 服务器的服务功能被抑制。

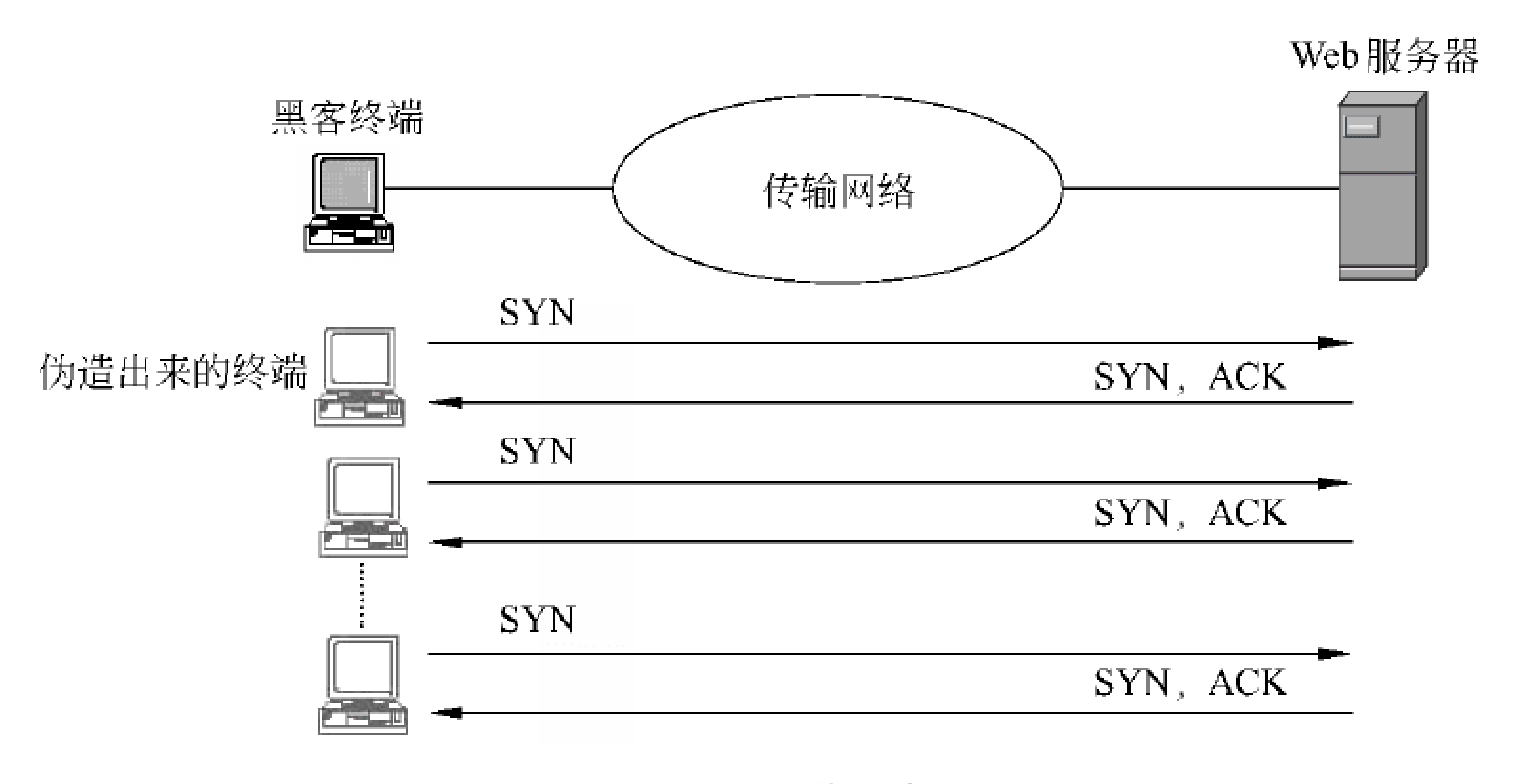


图 2.6　SYN 泛洪攻击过程

2. Smurf 攻击

Smurf 攻击过程如图 2.7 所示，黑客终端发送一个以被攻击终端的 IP 地址为源 IP 地址，定向广播地址为目的 IP 地址的 ICMP ECHO 请求报文，定向广播地址是网络号为某个特定网络的网络号，主机号全 1 的 IP 地址，以这种地址为目的 IP 地址的 IP 分组将发送给网络号所指定网络中的全部终端，假定 LAN 1 的网络号为 192.1.1.0/24，黑客终端的 IP 地址为 192.1.1.1，LAN 2 的网络号为 192.1.2.0/24，被攻击终端的 IP 地址为 192.1.2.1，LAN 3

和 LAN 4 的网络号分别为 10.1.0.0/16 和 10.2.0.0/16，黑客终端发送给 LAN 3 的 ICMP ECHO 请求报文的源 IP 地址为 192.1.2.1，目的 IP 地址为 10.1.255.255。这样的 IP 分组在 LAN 3 中以广播方式传输，到达 LAN 3 中的所有网络终端。由于接收到的是 ICMP ECHO 请求报文，LAN 3 中所有网络终端生成并发送以自身 IP 地址为源 IP 地址，ICMP ECHO 请求报文的源 IP 地址为目的 IP 地址的 ICMP ECHO 响应报文，这些 IP 分组一起发送给被攻击终端，导致被攻击终端和 LAN 3 之间的数据传输通路发生拥塞，使得其他网络中的终端无法和被攻击终端正常通信。黑客终端能够阻塞掉被攻击终端连接网络的链路的主要原因是利用了目标网络的放大作用，由于定向广播地址的接收方是特定网络中的所有网络终端，因此，黑客终端发送的单个 ICMP ECHO 请求报文将引发特定网络中的所有终端向被攻击终端发送 ICMP ECHO 响应报文，如果该特定网络中有 100 个终端，黑客终端发送的攻击报文就被放大了 100 倍。如图 2.7 所示，在 LAN 3 和 LAN 4 分别连接三个网络终端的情况下，黑客终端发送的两个 ICMP ECHO 请求报文导致被攻击终端接收到六个 ICMP ECHO 响应报文。

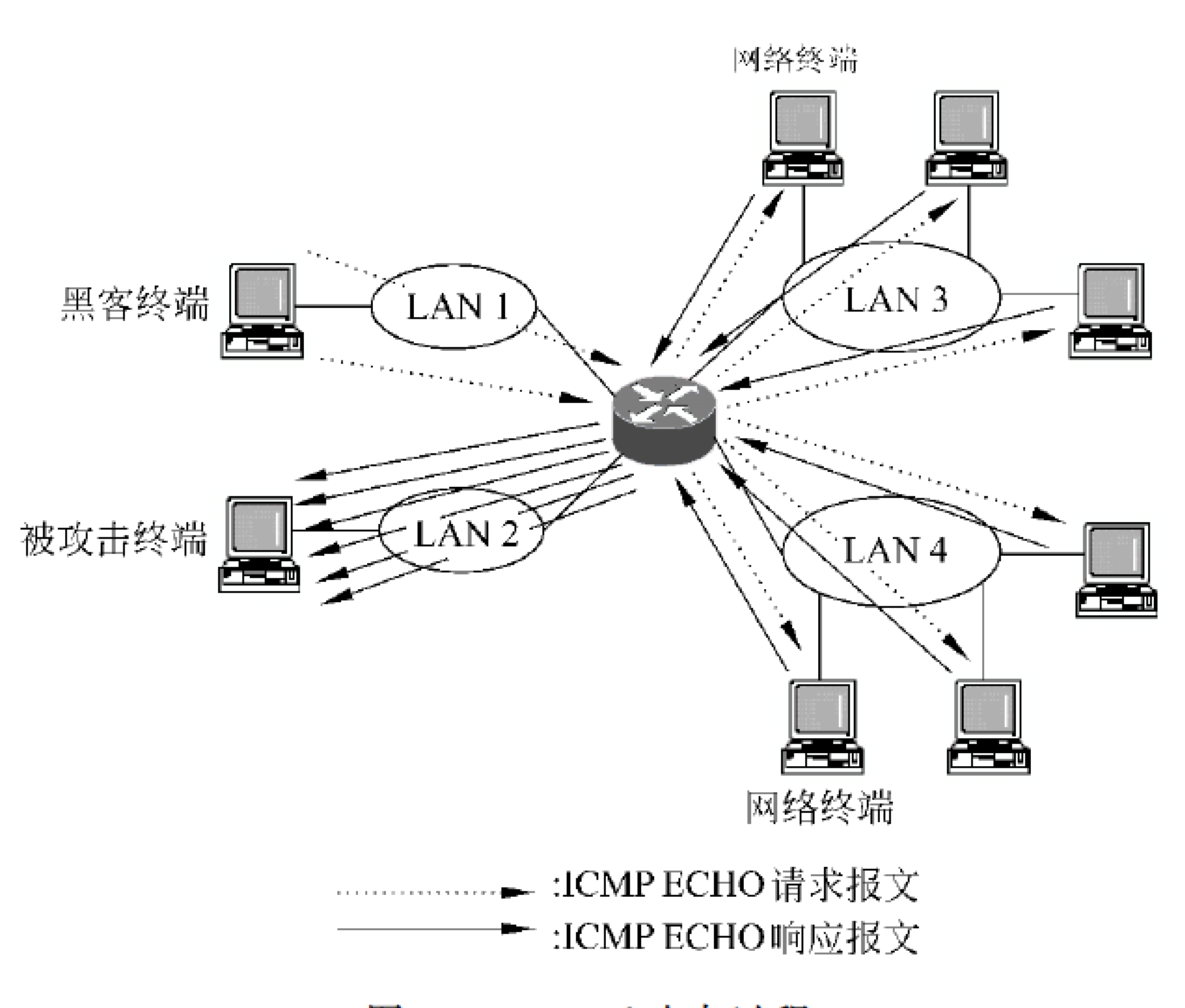


图 2.7 Smurf 攻击过程

2.1.4 恶意代码

1. 恶意代码分类

恶意代码分类的标准主要是代码的独立性和自我复制性。独立的恶意代码是指具备一个完整程序所应该具有的全部功能，能够独立传播、运行的恶意代码，这样的恶意代码不需要寄宿在另一个程序中。非独立恶意代码只是一段程序，它必须嵌入某个完整的程序中，作为该程序的一个组成部分进行传播和运行。具有自我复制能力的恶意代码是指能够自动将自己传染给其他程序(非独立恶意代码)或者传播给其他系统(独立恶意代码)的恶意代码。不具有自我复制能力的恶意代码必须借助其他媒介进行传播。目前具有的

恶意代码种类及属性如图 2.8 所示。按照图 2.8 中的分类称为病毒的恶意代码，称之为狭义病毒，习惯上，把特洛伊木马、病毒、蠕虫和 Zombie 统称为病毒，为和狭义病毒相区别，将这种病毒称为广义病毒。

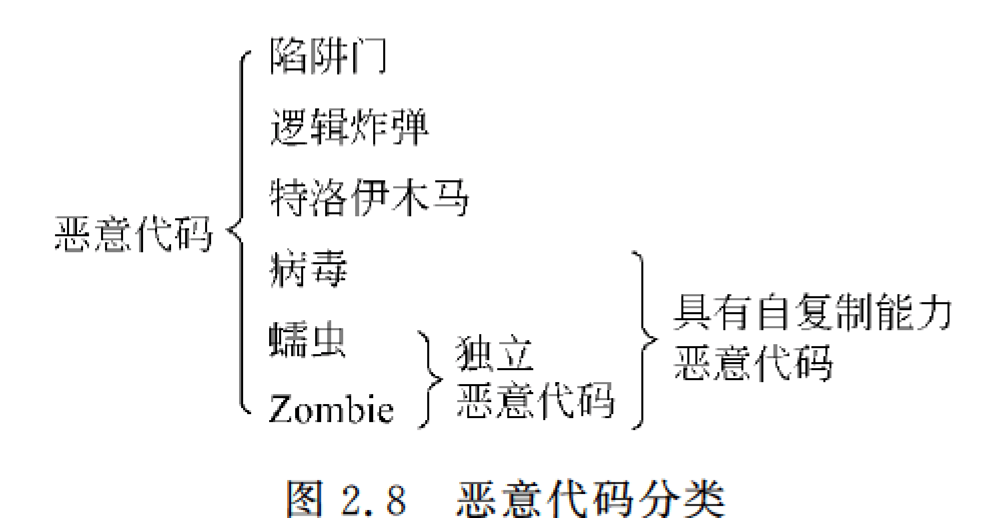


图 2.8　恶意代码分类

2. 病毒结构

病毒的广义定义是一切具有自我复制能力的恶意代码，这也是习惯上病毒的含义。图 2.9 是寄生在某个正常实用程序中的病毒结构，在这个结构中，病毒部分被添加在实用程序的前面，它主要由感染子程序、破坏子程序和激发条件测试子程序三部分组成。感染子程序的功能是将一个正常实用程序变成图 2.9 所示的病毒结构，为了避免多次重复感染，感染后的实用程序被添加感染标记 1234567；破坏子程序完成任何设定的破坏功能，如删除文件和数据、在系统登录程序中设置后门等；激发条件测试子程序用于测试激发破坏子程序的条件是否成立，如果成立，则返回真，否则，返回假。从图 2.9 所示的病毒结构可以看出，在正常执行原来的实用程序前，它首先执行感染子程序，然后测试激发破坏子程序的条件是否成立，并在返回值为真的情况下，执行破坏子程序，完成这些操作后，才真正开始执行实用程序。

```
program V:=
{goto main;
1234567;
       subroutine infect-executable:=
          {loop;
            file:=get-random-executable-file;
            if(first-line-of-file=1234567)
                then goto loop
                else prepend V to file;}
         subroutine do-damage:=
            {whatever damage is to be done}
         subroutine trigger-pulled:=
            {return true if some condition holds}
}
main:   main-program:=
{
              {infect-executable;
                if trigger-pulled then do-damamge;
                goto next;}
next:
}
```

图 2.9　病毒结构

一旦运行一个感染了病毒的实用程序，病毒就会感染其他实用程序，在某个条件出现

之前,病毒一般不会执行破坏子程序,在执行破坏子程序前,病毒不会对系统造成实质性的损害。激发病毒执行破坏子程序的条件随病毒不同而不同,有的用日期作为激发条件,有的用特定的操作序列作为激发条件,有的甚至用病毒的复制次数作为激发条件。

从图 2.9 所示的病毒结构,可以得出病毒的四个阶段。

(1) 静寂阶段:感染病毒的实用程序没有处于运行状态,病毒对系统没有影响。

(2) 传播阶段:运行感染病毒的实用程序,使系统中的其他实用程序感染病毒,但没有出现激发执行破坏子程序的条件,因此,只是使系统感染病毒,还没有对系统造成实质性的伤害。

(3) 触发阶段:创造激发执行破坏子程序的条件,如果条件是特定操作序列,触发阶段就是完成特定操作序列的阶段。

(4) 执行阶段:出现激发执行破坏子程序的条件,开始执行破坏子程序,完成对系统的破坏操作,如删除文件、数据等。

为了保证病毒的运行,并在出现激发执行破坏子程序的条件时,立即对系统进行破坏操作,存在多种触发病毒的方式。

- 寄生在实用程序中:这是一种常见的触发病毒的方式,病毒寄生在实用程序中,运行实用程序即运行病毒。但只能通过运行包含病毒的实用程序才能触发病毒,病毒随着实用程序的执行结束回到静寂阶段。
- 常驻内存:病毒寄生在某个实用程序中,一旦运行包含病毒的实用程序,病毒将常驻内存,不随着实用程序的结束而退出内存,病毒一直在后台运行,在出现激发执行破坏子程序的条件时,立即对系统进行破坏操作。
- 寄生在引导程序中:病毒如果寄生在某个实用程序中,需要运行感染病毒的实用程序才能初次激发病毒。如果病毒寄生在引导程序中,则每一次引导系统时都将触发病毒。

对于图 2.9 所示的病毒结构,感染病毒的实用程序的长度大于实用程序的原始长度,这将成为检验某个实用程序是否感染病毒的依据,为了增强病毒的隐蔽性,通常采用图 2.10所示的病毒结构。在将病毒程序添加到某个实用程序前,先压缩该实用程序,保证压缩后实用程序的长度和病毒程序长度之和等于实用程序的原始长度。在运行实用程序时,和图 2.9 所示的病毒结构一样,先运行病毒程序,然后解压并运行实用程序。

3. 常见恶意代码介绍

1) 陷阱门

陷阱门是某个程序的秘密入口,通过该入口启动程序,可以绕过正常的访问控制过程,因此,获悉陷阱门的人员可以绕过访问控制过程,直接对资源进行访问。陷阱门已经存在很长一段时间,原先的作用是程序员开发具有认证或登录过程的应用程序时,为避免每一次调试程序时都需输入大量认证或登录过程需要的信息,通过陷阱门启动程序的方式,来绕过认证或登录过程。程序区别正常启动和通过陷阱门启动的方式很多,如携带特定的命令参数,在程序启动后输入特定字符串等。

程序设计者是最有可能设置陷阱门的人,因此,许多免费下载的实用程序中含有陷阱门或病毒这样的恶意代码,使用免费下载的实用程序时必须注意这一点。

```
program V:=
{goto main;
1234567;
     subroutine infect-executable:=
       {loop;
        file:=get-random-executable-file;
        if(first-line-of-file=1234567) goto loop
           compress file;
           prepend V to file;}
      subroutine do-damage:=
        {whatever damage is to be done}
      subroutine trigger-pulled:=
        {return true if some condition holds}
}
main:  main-program:=
{
         {infect-executable;
          if trigger-pulled then do-damamge;
          goto next;}
next:     uncompress rest-of-file;
}
```

图 2.10 增强隐蔽性的病毒结构

2）逻辑炸弹

逻辑炸弹是包含在正常应用程序中的一段恶意代码，当某种条件出现，如到达某个特定日期，增加或删除某个特定文件等，将激发这一段恶意代码，执行这一段恶意代码将导致非常严重的后果，如删除系统中的重要文件和数据，使系统崩溃等。历史上不乏程序设计者利用逻辑炸弹讹诈用户和报复用户的案例。

3）特洛伊木马

特洛伊木马也是包含在正常应用程序中的一段恶意代码，一旦执行这样的应用程序，将激发恶意代码。顾名思义，这一段恶意代码的功能主要在于削弱系统的安全控制机制，如在系统登录程序中加入陷阱门，以便黑客能够绕过登录过程直接访问系统资源；将共享文件的只读属性修改为可读写属性，以便黑客能够对共享文件进行修改；甚至允许黑客通过远程桌面这样的工具软件控制系统。

4）病毒

这里的病毒是狭义上的恶意代码类型，单指那种既具有自我复制能力，又必须寄生在其他实用程序中的恶意代码。它和陷阱门、逻辑炸弹的最大不同在于自我复制能力，通常情况下，陷阱门、逻辑炸弹不会感染其他实用程序，而病毒会自动将自身添加到其他实用程序中。如果特洛伊木马也是寄生在实用程序中的一段恶意代码，那么，它就是一种病毒。

5）蠕虫

从病毒的广义定义来说，蠕虫也是一种病毒，但它和狭义病毒的最大不同在于自我复

制过程，病毒的自我复制过程需要人工干预，无论运行感染病毒的实用程序，还是打开包含宏病毒的邮件，都不是由病毒程序自我完成的。蠕虫能够自我完成下述步骤：

- 查找远程系统：能够通过检索已被攻陷的系统的网络邻居列表或其他远程系统地址列表找出下一个攻击对象。
- 建立连接：能够通过端口扫描等操作过程自动和被攻击对象建立连接，如 Telnet 连接等。
- 实施攻击：能够自动将自身通过已经建立的连接复制到被攻击的远程系统，并运行它。

6）Zombie

Zombie 是一种具有秘密接管其他连接在网络上的系统，并以此系统为平台发起对某个特定系统的攻击的功能的恶意代码。Zombie 主要用于定义恶意代码的功能，并没有涉及该恶意代码的结构和自我复制过程，因此，分别存在符合狭义病毒的定义和蠕虫定义的 Zombie。

4. 病毒传播过程

1）通过移动媒介进行传播

在网络普及之前，病毒主要通过移动媒介进行传播，假定 A 系统中执行了某个感染了病毒的实用程序，病毒将感染 A 系统中的其他可执行文件，如果某个用户通过移动媒介将 A 系统中某个感染了病毒的可执行文件复制到 B 系统，并执行该可执行文件，B 系统中其他可执行文件也将被该病毒感染。如果该病毒被激发后，常驻内存，当某个移动媒介作为 A 系统的一部分后，即使从 A 系统中复制的文件没有被感染病毒，在向移动媒介复制文件的过程中，病毒也可能感染移动媒介中的其他可执行文件，一旦在 B 系统执行这些感染了病毒的可执行文件，病毒同样将感染 B 系统。

2）通过 Web 站点进行传播

在网络得到普及后，网络成为传播病毒的主要途径，一些别有用心的人常常在一些 Web 站点提供包含恶意代码的实用程序供用户免费下载，用户一旦下载并运行了这样的实用程序，系统便被感染了病毒。由于这些实用程序的功能非常有用，导致下载的用户很多，使病毒快速传播。一些喜欢开发一些实用程序的程序设计者由于没有通过开发的实用程序获得正当赢利，常常被一些别有用心的人利用，在开发的实用程序中加入恶意代码。这种传播方式目前十分普遍，用户必须对免费下载的实用程序抱有警惕。

目前，Web 站点提供的不仅仅是静态 HTML 文档，还可以提供嵌入了 Java 小应用程序（applet）的活动 HTML 文档，浏览器提供的 Java 运行环境（Java 虚拟机）能够执行嵌入在 HTML 文档中的 Java 小应用程序，用户和 Web 服务器以此实现交互过程。但活动 HTML 文档也给病毒传播带来了便利，许多病毒设计者将病毒作为 Java 小应用程序嵌入在 HTML 文档中，一旦某个用户链接了这样的活动 HTML 文档，病毒将感染该系统。

3）通过电子邮件进行传播

通过在电子邮件的附件中插入病毒程序来传播病毒是网络普及后又一常见的病毒传播方式。当用户打开附件后，系统执行附件中的病毒程序，该病毒程序通过检索系统的地

址簿，以地址簿中的所有地址为接收者转发该邮件。由于用户看到的邮件发送地址是熟悉的邮件地址，常常放心地打开邮件附件，导致系统被病毒感染，并使病毒进一步去感染其他系统，使该病毒快速传播。

随着宏病毒的出现，邮件正文可以包含宏病毒，对于邮件正文包含宏病毒的邮件，只要用户打开邮件，宏病毒将感染系统，并进一步去感染其他系统。

4）自动传播

通过电子邮件传播宏病毒的方式不能算是自动传播，因为，只有打开邮件正文包含宏病毒的邮件，才能激发宏病毒，而宏病毒自身是无法自动完成这一过程的。按照蠕虫的定义，蠕虫一旦激发，它不但可以将自身复制给其他系统，并且能够在其他系统中运行该蠕虫病毒，这是蠕虫病毒能够快速传播的主要原因。

2.2　黑客攻击过程

2.2.1　收集信息

在对某个主机系统或某个网络实施攻击前，首先必须了解该主机系统或该网络，对于主机系统，必须知道运行的操作系统类型、版本，运行的服务器软件类型、版本，提供的服务类型等，对于网络，必须了解网络接入方式、网络拓扑结构、交换机或路由器生产厂家及类型等，黑客收集信息过程就是获取上述信息的过程。

1. 网络接入方式

如果攻击的主机系统连接在内部网络上，首先需要了解内部网络的接入方式，通常情况下，终端接入网络的方式有三种：公共交换电话网（Public Switched Telephone Network，PSTN）拨号接入、无线局域网接入和以太网接入。以太网接入必须完成物理连接过程，对于保安设施较完善的企业，黑客直接将终端连接到内部网络中某个以太网交换机端口是一件比较困难的事情，因此，要通过各种渠道了解内部网络是否存在PSTN拨号接入或无线局域网接入方式。

2. 主机系统信息

在对主机系统实施攻击前，必须了解主机系统使用的操作系统类型（Windows、UNIX或Linux）、操作系统版本、主机系统提供的服务类型（Web服务、FTP服务和邮件服务）、系统服务器软件类型（IIS或Apache），以及其他有关主机系统的信息。

3. 网络拓扑结构

在对主机系统实施攻击前，另一种必须了解的信息是有关黑客终端至被攻击主机系统的数据传输路径的信息，它包含传输路径上设备的类型（交换机、路由器、防火墙、入侵防御系统等）、设备的生产厂家，构成传输路径的各个传输网络类型等。

2.2.2　侦察

侦察的目的是寻找到将攻击信息传输给被攻击主机系统的方法，找出被攻击主机系统的缺陷。

1. 被攻击主机系统的 IP 地址

获得被攻击主机系统的完全合格的域名或 IP 地址。

2. 了解防火墙配置及绕过防火墙的方法

如果在黑客终端和被攻击主机系统之间存在防火墙，必须了解防火墙的安全策略，攻击信息利用安全策略漏洞穿过防火墙的方法。

3. 主机系统软件缺陷

根据信息收集阶段获得的被攻击主机系统的操作系统类型、版本（如 Windows Server 2003），提供的服务类型（如 Web 服务），服务器软件的类型（如 Apache httpd），找出这些系统软件已被发现的缺陷，并测试这些缺陷是否已经全部通过补丁软件得到弥补。

4. 端口扫描

通过端口扫描找出被攻击主机系统允许建立 TCP 连接的端口号，并通过在这些端口号建立 TCP 连接，以这些 TCP 连接为管道对被攻击主机系统实施攻击。

5. 是否感染特洛伊木马

如果被攻击主机系统已经感染了某种已知的特洛伊木马病毒，将使攻击变得容易。

2.2.3 攻击

在成功接入网络并了解攻击目标的相关信息后，黑客可以开始对攻击目标的攻击过程，如通过拒绝服务攻击瘫痪攻击目标，或是利用攻击目标的漏洞上载恶意代码，黑客可以自己编写用于攻击的工具软件，也可以使用业已存在的大量黑客工具软件。

2.3 黑客攻击实例

2.3.1 内部网络结构

图 2.11 是黑客准备攻击的内部网络结构，它由三个局域网组成：无线局域网、以太网 LAN 1 和 LAN 2。黑客的攻击目标是使内部网络中的 Web 服务器丧失服务能力，并篡改 Web 服务器中的数据。

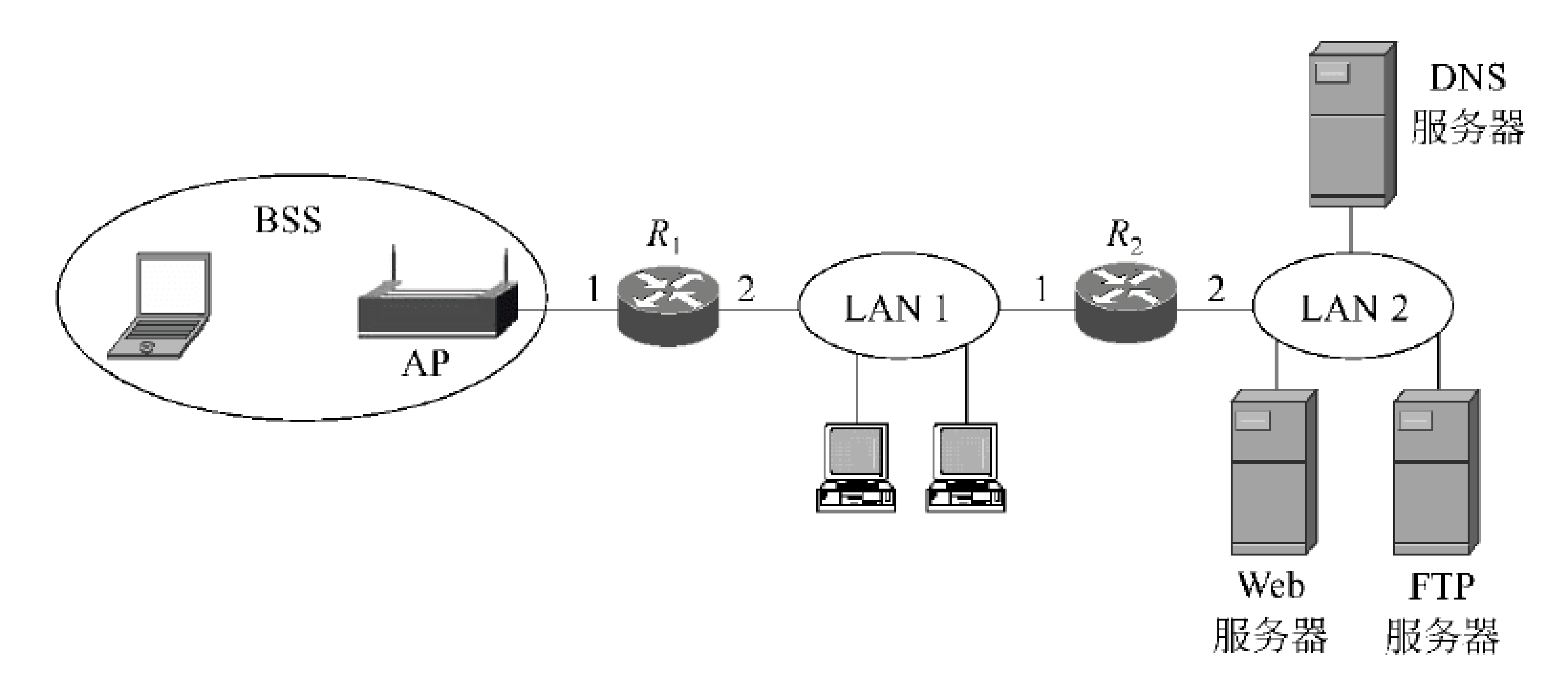


图 2.11 内部网络结构

2.3.2 非法接入

黑客通过移动终端接入图 2.11 所示的无线局域网需要完成三个过程：同步过程、认证过程和建立关联过程。黑客终端通过同步过程获得 AP MAC 地址、所使用的信道、物理层标准及双方均支持的数据传输速率。通过认证过程使黑客终端成为合法的 BSS 工作站，通过建立关联过程完成无线局域网的接入，因此，无线局域网建立关联过程的功能相当于总线型以太网的物理接入，BSS 中只有 MAC 地址包含在 AP 关联表中的终端才能实现和 AP 的数据交换。黑客终端完成这三个过程必须解决两个问题：一是必须获得 BSS 的 SSID，二是必须通过共享密钥认证机制下的认证过程。

1. 获得 SSID

AP 周期性地公告信标帧，信标帧中以明文方式给出 AP 的服务集标识符（Service Set Identifier，SSID），因此，只要通过侦听 AP 公告的信标帧，就可获得 AP 的 SSID。虽然有些 AP 作为可选项可以屏蔽掉信标帧中的 SSID，但必须在探测响应帧中以明文方式给出 SSID，因此，黑客终端可以通过侦听信标帧或探测响应帧获得 AP 的 SSID。

如图 2.12 所示，授权终端或者通过侦听 AP 发送的信标帧，或者通过和 AP 交换探测请求和响应帧完成同步过程，由于无线电通信的开放性，黑客终端可以侦听到授权终端和 AP 之间在同步过程中交换的 MAC 帧，并因此获得 SSID。

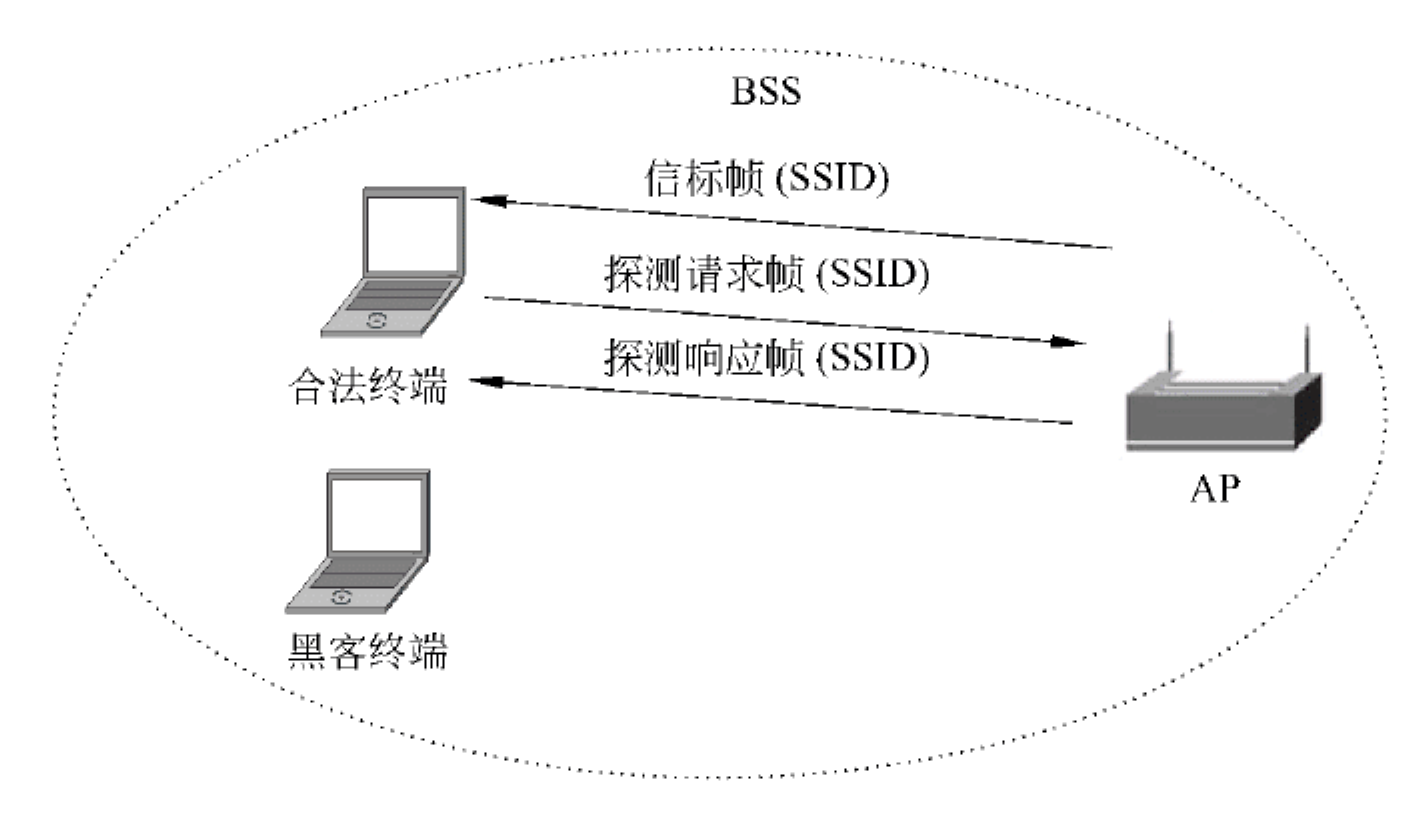


图 2.12　获得 SSID 过程

2. 完成共享密钥认证机制下的认证过程

1）共享密钥认证机制

共享密钥认证机制的思路是为所有授权终端分配一个共享密钥 GK，AP 和某个终端是否建立关联的依据就是该终端是否拥有共享密钥 GK，为了判别某个终端是否拥有共享密钥 GK，AP 先向其发送一个固定长度的随机数 challenge，终端以共享密钥 GK 和初始向量 IV 为随机数种子，通过随机数生成函数 PRF 生成一个和随机数 challenge 相同长度的随机数 K（$K=\text{PRF}(\text{GK},\text{IV})$），用 K 异或随机数 challenge，并将异或操作结果 Y（$Y=\text{challenge}\oplus K$）和初始向量 IV 一同发送给 AP，AP 同样以共享密钥 GK 和发送端以明文方式发送的初始向量 IV 为随机数种子，通过相同的随机数生成函数 PRF 生成一

个和随机数 challenge 相同长度的随机数 K'(K'=PRF(GK,IV)),如果 $K=K'$,意味着AP 和该终端拥有相同的共享密钥 GK。AP 判别 K 是否等于 K' 的方法是用 K' 异或发送端发送的密文 Y,如果异或运算结果等于随机数 challenge,表明 K 等于 K'。因为如果 K 等于 K',则 $K \oplus Y = K \oplus \text{challenge} \oplus K = \text{challenge}$。随机数生成函数 PRF 必须保证所生成的随机数和随机数种子一一对应,同时用共享密钥 GK 和初始向量 IV 作为随机数种子是为了在共享密钥 GK 不变的情况下,通过改变初始向量 IV,改变和随机数 challenge 异或的随机数 K。

2) 黑客终端欺骗 AP 过程

如果黑客终端想通过 AP 共享密钥认证机制下的认证过程,就会进行如图 2.13 所示的操作。黑客终端一直侦听其他授权终端进行的共享密钥认证机制下的认证过程,由于无线电通信的开放性,黑客终端可以侦听到授权终端和 AP 之间在认证过程中相互交换的所有认证请求/响应帧。AP 发送给授权终端的认证响应帧中给出固定长度的随机数 P,授权终端发送给 AP 的认证请求帧中给出密文 Y 和初始向量 IV,其中密文 $Y = P \oplus K$,K=PRF(GK,IV)。由于黑客终端侦听到了 AP 以明文方式发送给授权终端的随机数 P、授权终端发送给 AP 的对随机数 P 加密后的密文 Y 和明文方式给出的初始向量 IV,黑客终端完全可以得出授权终端用于此次加密的一次性密钥 K 和对应的初始向量 IV,$K = P \oplus Y = P \oplus P \oplus K$。当黑客终端希望通过 AP 认证时,它也发起认证过程,并用侦听到的一次性密钥 K 加密 AP 给出的随机数 P',并将密文 Y' 和对应的初始向量 IV 封装在认证请求帧中发送给 AP,其中 $Y' = P' \oplus K$。由于黑客终端使用的一次性密钥 K 和初始向量 IV 都是有效的,即 K=PRF(GK,IV),AP 通过对黑客终端的认证,即错误地认为黑客终端拥有共享密钥 GK。

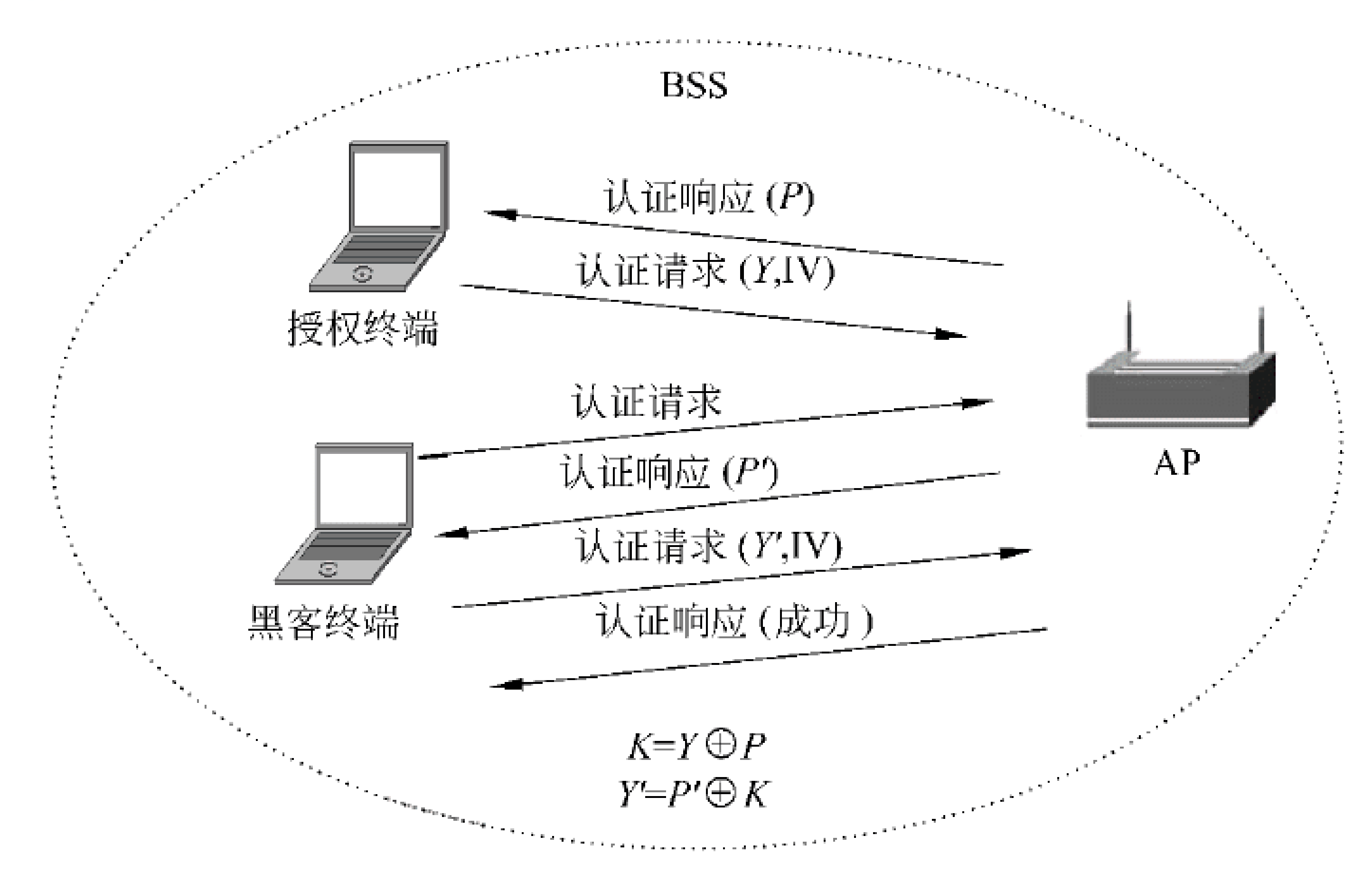


图 2.13 黑客终端通过 AP 认证的过程

2.3.3 获取 DNS 服务器内容

黑客终端对内部网络实施攻击前,必须先了解内部网络的服务器配置,而 DNS 服务器的内容完整给出了服务器域名和 IP 地址之间的绑定关系。因此,只要获得内部网络

DNS服务器的内容,就可了解内部网络的服务器配置。

通过域名系统(Domain Name System,DNS)服务器的区域传送操作获得内部DNS服务器的内容。区域传送操作指的是一台后备DNS服务器用来自主DNS服务器的数据刷新自己的区域数据库,这一操作的主要目的是为运行中的DNS服务提供一定的冗余度,避免因为主DNS服务器发生故障而导致网络系统崩溃。正常情况下,区域传送操作只有在网络中真的存在后备DNS服务器时,才需要执行,但许多DNS服务器被错误配置成只要有用户发出请求,就会向对方提供一个区域数据库的备份。这样,黑客终端可以通过执行命令nslookup将内部网络DNS服务器的内容重定向到某个文件中。

2.3.4 拒绝服务攻击

1. 获取网络拓扑结构

假定在内部DNS服务器中检索到如下信息:

```
www.abc.com    IN    A    192.168.1.1
ftp.abc.com    IN    A    192.168.1.2
dns.abc.com    IN    A    192.168.1.3
```

获知内部网络中存在三个服务器,它们分别是Web服务器、FTP服务器和DNS服务器,及这三个服务器对应的IP地址。在获知Web服务器的IP地址后,可以通过traceroute工具(在Windows操作系统中,traceroute工具的程序名为tracert)找出黑客终端至Web服务器的数据传输路径。针对图2.11所示的网络拓扑结构,获得黑客终端至Web服务器的数据传输路径为192.168.3.2(黑客终端IP地址)→192.168.3.254(路由器R_1端口1 IP地址)→192.168.2.254(路由器R_2端口1 IP地址)→192.168.1.1(Web服务器IP地址)。

2. Smurf攻击

在获取了内部网络的拓扑结构后,黑客终端可以通过Smurf攻击使Web服务器丧失服务能力。攻击过程如图2.14所示,黑客终端构建一个ICMP ECHO请求报文,并将该报文封装在以Web服务器IP地址(192.168.1.1)为源IP地址,以定向广播地址192.168.2.255为目的IP地址的IP分组中,该IP分组经过路由器R_1转发后,在LAN 1内广播,使LAN 1

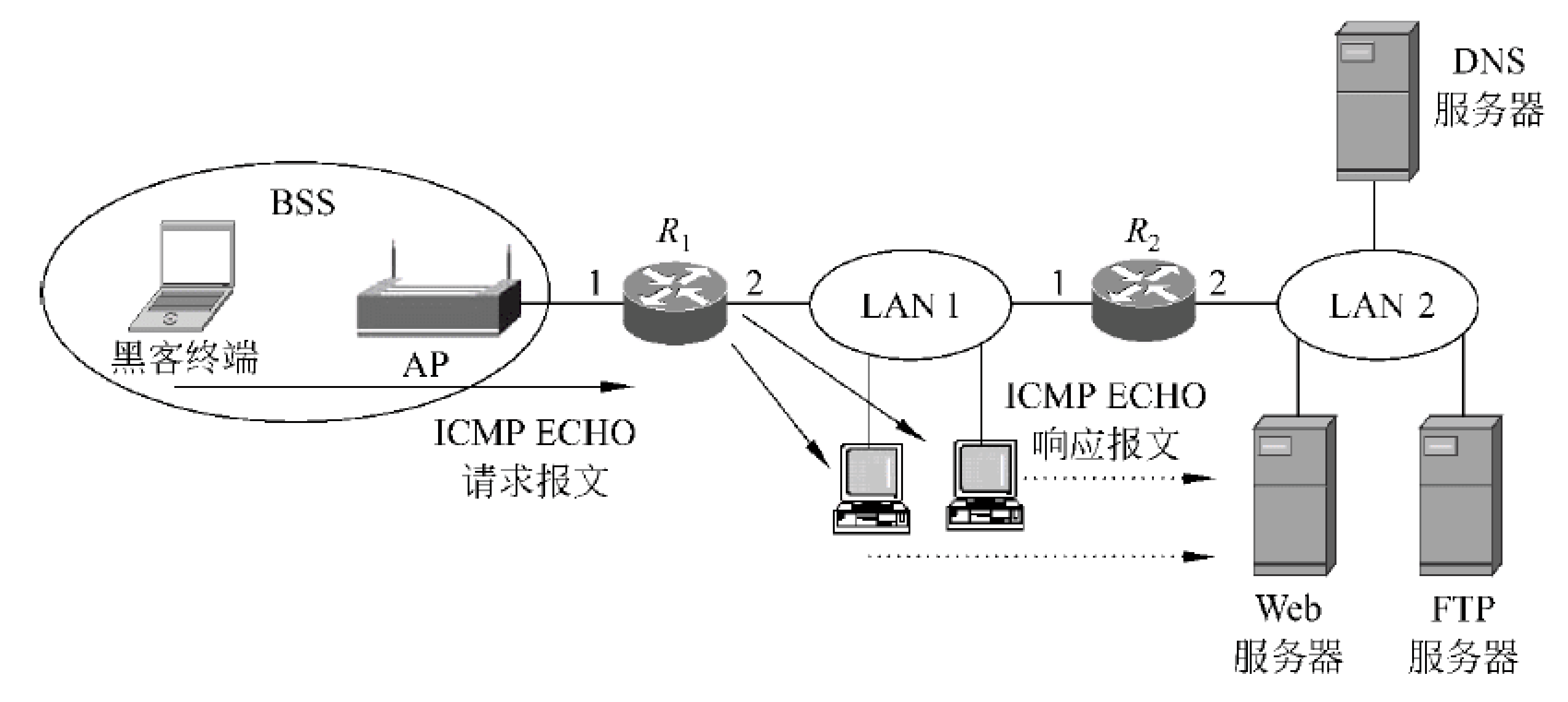


图2.14 黑客终端对Web服务器实施Smurf攻击的过程

内的所有终端都接收到该 IP 分组，并向由该 IP 分组源 IP 地址指定的终端发送 ICMP ECHO 响应报文。在 LAN 1 内存在大量终端的情况下，Web 服务器的处理能力及连接 LAN 2 的链路的带宽都将被这些 ICMP ECHO 响应报文耗尽，导致 Web 服务器无法对正常的 HTTP 请求报文作出响应。

2.3.5 非法访问

1. 获取 Web 服务器的可执行脚本

Web 服务器中的可执行脚本原本应该在 Web 服务器上被调用执行，不应该发送到客户端，但 Web 服务器功能块中的漏洞允许黑客下载完整的可执行脚本文件，如 Translate:f 漏洞攻击。

黑客终端向 Web 服务器发送一个精心构造的 HTTP GET 请求：

```
GET/global.asa\HTTP/1.0
HOST:192.168.3.2
Translate:f
[CRLF]
[CRLF]
```

这个 HTTP GET 请求导致 Web 服务器直接将 global. asa 文件发送给黑客终端，由于许多站点习惯把应用程序的口令存放在 global. asa 文件中，因此，当黑客获得global. asa文件后，可以据此对其他应用程序展开攻击。

2. 缓冲区溢出

缓冲区溢出过程如图 2.15 所示，图左边是正常的缓冲区分配结构，由于函数 *B* 使用缓冲区时没有检测缓冲区边界这一步，当输入数据超过正常长度时，函数 *B* 的缓冲区发生溢出，超长数据将继续占用其他存储空间，覆盖用于保留函数 *A* 的返回地址的存储单元。如果黑客终端知道某个 Web 服务器功能块中存在缓冲区溢出漏洞，即该功能块使用缓冲区时，不检测缓冲区边界，黑客终端可以精心设计发送给该功能块处理的数据，如图 2.15右边所示，黑客终端发送给该功能块的数据中包含某段恶意代码，而且，用于覆盖函数 *A* 返回地址的数据恰恰是该段恶意代码的入口地址，这样，当系统返回到函数 *A* 时，实际上是开始运行黑客终端上传的恶意代码，由该恶意代码完成对系统的破坏功能，如删除或修改系统中的文件。

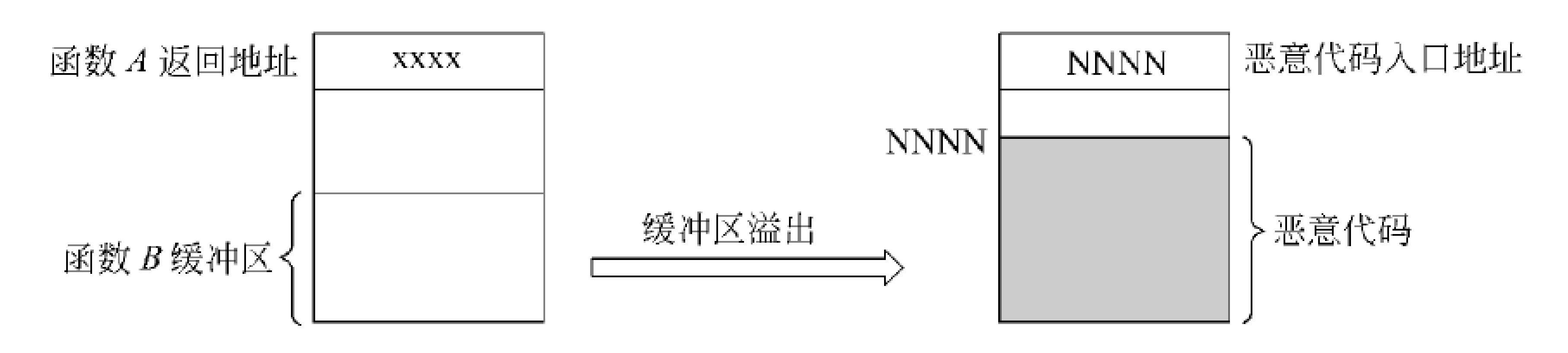


图 2.15 缓冲区溢出

Web 服务器中存在缓冲区溢出漏洞的功能块很多，因此，利用缓冲区溢出漏洞对 Web 服务器实施攻击是黑客的主要攻击手段。

2.4　网络安全和抑制黑客攻击

信息安全由网络安全、操作系统安全和应用程序安全三部分组成,因此,黑客攻击也是通过利用这三种安全存在的漏洞实现的,所以,只有彻底解决这三种安全存在的漏洞,才能完全杜绝黑客攻击。黑客攻击和信息安全是矛盾的两个方面,信息安全技术的发展对黑客攻击技术提出了更高的要求,因而促使黑客攻击技术的发展,同样,黑客攻击技术的发展,也促使信息安全技术的提高,因此,未来很长一段时间,信息安全技术和黑客攻击技术将相互竞争,相互促进,没有一种信息安全技术可以一劳永逸地解决信息安全问题。

构建一个安全网络是抑制黑客攻击的关键,无论是针对网络安全漏洞的黑客攻击过程,还是针对操作系统和应用程序安全漏洞的黑客攻击过程,都可通过增强网络的安全性得以解决或者缓解。

2.4.1　消除网络安全漏洞

通过增强网络的安全性解决或者缓解针对网络安全漏洞的黑客攻击,如通过安全路由技术解决黑客篡改路由表中路由项的问题,通过802.11i和802.1X安全技术解决黑客通过无线局域网和以太网非法接入内部网络的问题,通过信息流管制技术解决黑客用耗尽网络带宽使服务器丧失服务能力的拒绝服务攻击,通过VPN和加密技术解决黑客窃取信息和追踪信息源的问题,通过防火墙解决黑客非法访问敏感信息的问题,因此,网络安全技术必须为网络增加一层用于抵御黑客攻击的盔甲。

2.4.2　弥补操作系统和应用程序的安全漏洞

黑客利用操作系统和应用程序漏洞发起的攻击针对的往往是公开的应用服务器,如企业公开的Web服务器、著名网站等,这种情况下,黑客终端和被攻击目标之间的数据传输通路是畅通的,但网络安全技术可以通过检测它们之间传输的信息流模式,发现可能存在的攻击过程,并加以干预。如分布在网络关键网段和重要服务器上的入侵防御系统,就可检测出多种黑客利用操作系统和应用程序的安全漏洞进行的攻击过程,入侵防御系统不仅能够自动予以干预,还能向网络安全管理员报警。

习　题

2.1　给出几个已经发生的黑客攻击案例,说明这些攻击能够成功的技术和管理因素。

2.2　列出几个著名的黑客攻击工具软件,并分析这些工具软件的攻击机制。

2.3　以太网本身对信息窃取有什么防止技术?讨论这些技术解决信息窃取问题的机制。

2.4　IPv6如何解决地址解析问题?它的地址解析机制存在类似ARP欺骗问题吗?

2.5　拒绝服务攻击为什么难以解决?服务器能自己解决SYN泛洪攻击吗?试给

出网络解决拒绝服务攻击的方法。

2.6 用户终端常因为下载 Web 主页或服务器文件而感染病毒,用户终端自身有什么预防机制?网络能提供什么解决办法?

2.7 病毒传播机制是什么?为什么说网络是病毒的快速传播通道?

2.8 蠕虫病毒的传播机制和狭义病毒的传播机制有什么不同?

2.9 针对 2.3 节中给出的黑客攻击机制,试给出反制机制。

2.10 如何判定某个终端或网络正在被黑客侦察?如何反制黑客侦察?

2.11 隐真示假是战争中常见的伪装技术,网络中是否存在通过伪装技术实现防止黑客攻击的目标的方法?

2.12 内部网络中某个存在安全漏洞(操作系统漏洞或应用程序漏洞)的主机,往往成为黑客攻击内部网络的跳板,有什么办法可以消除这样的安全隐患?

2.13 笔记本电脑的移动特性使其经常成为病毒的传播中介,如何防止这一点?

2.14 主机防火墙配置对防止黑客攻击能起到什么作用?

2.15 参考 TCP 重传机制中辨别重复接收的 TCP 报文的方法,给出防止中继攻击的方法。

2.16 无线局域网的开放性对网络安全带来哪些挑战?如何解决?

2.17 一些木马软件窃取用户所有对话框中的输入数据,并发送给攻击者,攻击者从中获取用户私密信息。对这样的攻击手段有什么预防机制?

第3章 CHAPTER

网络安全基础

3.1 加密算法

加密是网络安全的基础，加密过程如图 3.1 所示，发送端通过加密算法 E 和加密密钥 K_1 将明文 P 转换成密文 $Y(Y=E_{K_1}(P))$，接收端通过解密算法 D 和解密密钥 K_2 重新将密文还原成明文 $P(P=D_{K_2}(Y)=D_{K_2}(E_{K_1}(P)))$。密文 Y 虽然和明文 P 相关联，在不知道解密算法 D 和解密密钥 K_2 的情况下，是无法通过密文 Y 解析出明文 P，因此，只要不让黑客获悉解密算法 D 和解密密钥 K_2，即使让黑客截获密文 Y，黑客也无法获得明文 P，因而也无法实现窃取信息的攻击目标。如果加密算法所使用的加密密钥 K_1 等于解密密钥 K_2，这种加密算法被称为对称密钥加密算法，否则，被称为不对称密钥加密算法，目前，常见的对称密钥加密算法有数据加密标准(Data Encryption Standard，DES)、高级加密标准(Advanced Encryption Standard，AES)，不对称密钥加密算法有 RSA(Rivest-Shamir-Adleman)公开密钥加密算法。

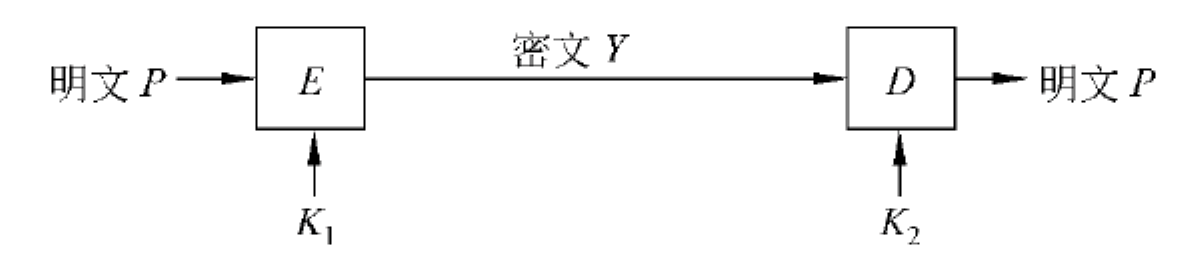


图 3.1 加密解密过程

3.1.1 对称密钥加密算法

对称密钥加密算法由五个元素组成：明文 P、密文 Y、加密算法 E、解密算法 D 和密钥 K(加密密钥 K_1 = 解密密钥 $K_2=K$)。由于加密算法和解密算法的运算过程是互逆的，因此，很容易从一种操作过程推出另一种操作过程，这样，密文 Y 的安全性就取决于加密算法和密钥的安全性。由于黑客可以截获到密文 Y，甚至可以得到一部分密文 Y 及对应的明文 P，对称密钥加密算法必须保证在黑客即使获得一部分密文Y及对应的明文

P 的条件下，也无法推导出加密算法和密钥。如果加密算法和密钥长期不变的话，黑客获得加密算法和密钥只是时间问题，为保证对称密钥加密算法的安全性，或者定期更换密钥 K，或者定期更换加密算法 E 及对应的解密算法 D。在目前互联网时代，大量用户之间需要实现动态安全传输，为了实现动态安全传输，两个用户之间必须动态同步加密算法和密钥，在用软件实现加密、解密运算过程的情况下，不同的加密、解密算法需要不同的用于实现对应运算过程的程序块，而密钥只是实现加密、解密算法的程序块的输入参数，因此，实现密钥动态同步比实现加密、解密算法动态同步要简单得多。基于这样的理由，往往采用公开的、标准的加密、解密算法，而把密文 Y 的安全性完全基于密钥的安全性。

加密体制的 Kerckhoff's 原则是：所有加密、解密算法都是公开的，保密的只是密钥。

一旦加密、解密算法公开，在黑客能够获得一部分密文 Y 及对应的明文 P 的条件下仍然保证密钥安全性的前提是：或者黑客无法在知道加密、解密算法的情况下，通过有限的密文 Y 及对应的明文 P 推导出密钥 K。或者每一个密钥只进行一次加密运算，而且每一个密钥都是从一个足够大的密钥集中随机产生，密钥之间没有任何相关性。第一种情况要求足够复杂的加密、解密运算过程，而且这种运算过程必须经过广泛测试，保证黑客无法破解，即无法通过有限的密文和明文对解析出密钥。第二种情况要求一次一密钥，而且密钥必须在足够大的密钥集中随机产生，确保密钥之间没有相关性，黑客无法从已知的有限密钥序列推导出下一次用于加密运算的密钥，但对加密、解密算法的复杂性没有要求。

1. 流密码体制

流密码体制就是一次一密钥的加密运算过程，如图 3.2 所示，发送端在密钥集中随机产生一个与明文 P 相同长度的密钥 K，密钥 K 和明文 P 进行异或运算后得到密文 Y。接收端用同样的密钥 K 和密文 Y 进行异或运算，还原出明文 P。如果密钥集足够大，每一次加密运算的密钥不同，且这些密钥之间不存在相关性，这种密码体制是最安全的。但一是密钥集总是有限的，二是计算机很难真正在密钥集中随机产生密钥，密钥之间无法做到没有任何相关性，三是发送端和接收端必须同步密钥。在这些限制下，流密码体制的安全性就打了折扣。图 3.3 是无线局域网 WEP 安全机制使用的加密、解密运算过程，用于发送端加密运算的密钥由伪随机数生成器产生，原始密钥 K 和初始向量 IV 作为伪随机数种子，为了使接收端产生相同的密钥，必须使接收端的伪随机数生成器输入相同的伪随机数种子，为了做到一次一密钥，每一次产生密钥时，必须对伪随机数生成器输入不同的随机数种子。在无线局域网 WEP 安全机制中，原始密钥 K 是发送端和接收端共同约定的，安全传输过程中是不变的，双方需要同步的只是初始向量 IV，发送端每一次必须选择不

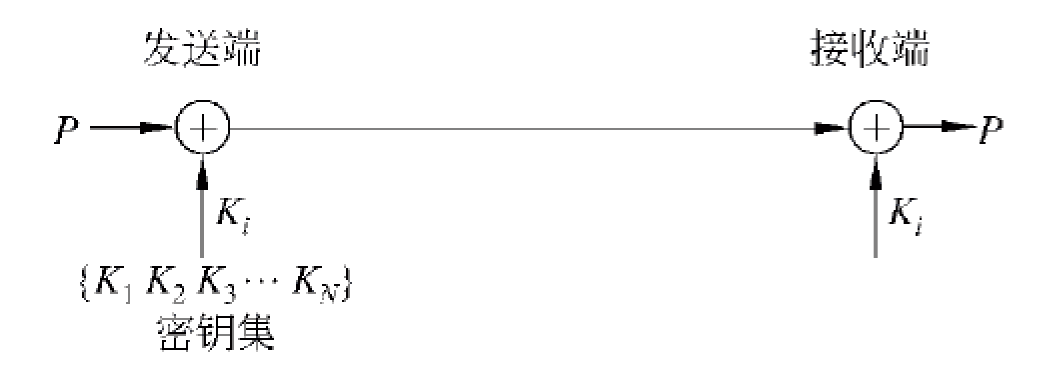


图 3.2 流密码体制加密、解密过程

同的初始向量作为伪随机数种子，并以明文方式将该次加密运算选择的初始向量发送给接收端。由于一是用伪随机数生成器来产生密钥，无法保证这些密钥之间没有任何相关性。二是作为伪随机数种子一部分的原始密钥 K 是不变的，增加了这些密钥之间的相关性。三是初始向量的长度只有 24 位，密钥集中的密钥数 $\leqslant 2^{24}$，如果原始密钥较长一段时间保持不变，加密用的密钥很容易重复。

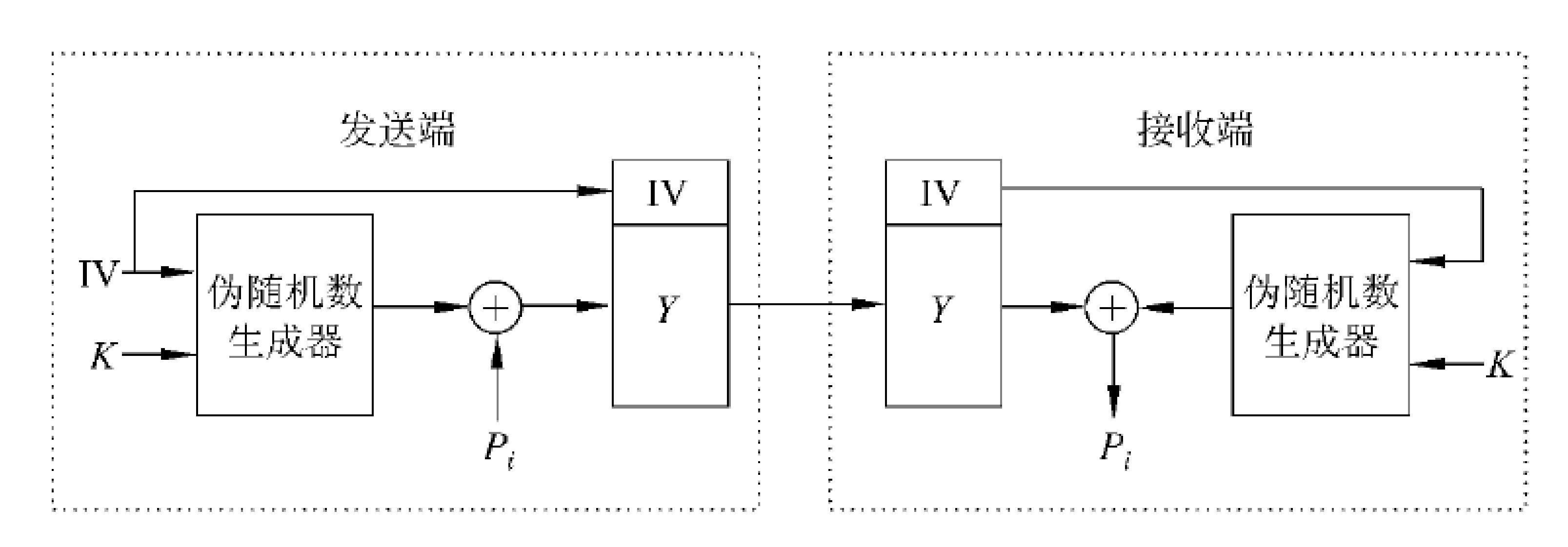


图 3.3　WEP 安全体制加密、解密过程

2. 分组密码体制

分组密码体制下，同一密钥用于多次加密运算过程，黑客可能截获这些用同一密钥加密后的密文，甚至可能获得了一部分密文对应的明文，加密、解密算法必须保证黑客无法通过密文，甚至有限的密文、明文对推导出密钥。这就要求分组密码体制下的加密、解密算法足够复杂，不能是流密码体制下简单的运算过程，因为类似图 3.3 所示的加密操作（异或运算）很容易让黑客根据密文、明文对推导出密钥（$Y=P\oplus K$. $P\oplus Y=P\oplus P\oplus K=K$）。分组密码体制下的加密运算过程，首先将明文分割成固定长度的数据组，然后单独对每一组数据进行加密运算，产生和数据组长度相同的密文，密文序列和明文分组后产生的数据组序列一一对应。解密运算过程就是将密文还原为对应数据组的过程。将数据组变成密文的加密过程通过多级操作完成，而每一级操作所进行的运算通常是替代与置换。

1）替代运算

替代是将数据组中的二进制数分段，每一段二进制数用对应的编码代替。假定 8 位数据组为 11010010，如果采用下述替代规则{00，110}，{01，010}，{10，000}，{11，100}，进行替代运算后的二进制位流为 100 010 110 000。当然，也可以用同样的替代规则完成反向替代运算，但必须指出：用二位二进制编码替代三位二进制编码的前提是三位二进制编码集包含的编码数量小于等于 4（二位二进制编码集的最大编码数量）。

2）置换运算

置换运算是按照置换规则重新排列数据组中二进制数的顺序，假定 8 位数据组为 11010010，如果置换规则为{0，2，5，7，3，1，6，4}，则数据组的置换运算过程如图 3.4 所示。置换规则中最高位对应值为 0，表明原来 8 位数据组中最高位被置换到第 0 位，第 6 位对应值为 2，表明原来 8 位数据组中第 6 位被置换到第 2 位，依此类推。

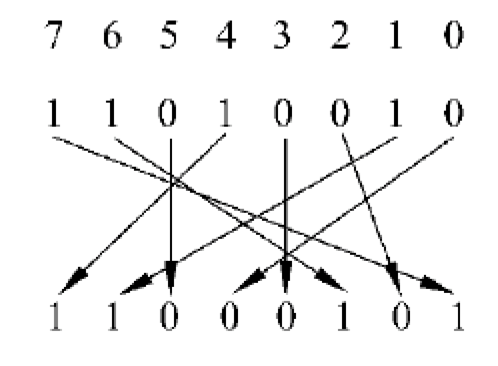


图 3.4　置换运算过程

3）Feistel 分组密码结构

Feistel 分组密码结构给出了分组密码体制下的加密运算过程，如图 3.5 所示，它的输入是分割明文后产生的长度固定为 2W 位的数据组和密钥 K，输出是 2W 位的密文。整个加密运算过程由 n 次迭代完成，上一次迭代运算的结果作为下一次迭代运算的输入，以密钥 K 为原始密钥经过子密钥生成运算产生各次迭代运算需要的子密钥集$\{K_1, K_2, \cdots, K_i, \cdots, K_n\}$。在第一次迭代运算中，数据组中的数据分成长度各为 W 位的左右两部分：L_0 和 R_0，R_0 和子密钥 K_1 作为迭代函数 F 的输入，迭代函数 F 的输出和 L_0 进行异或运算，运算的结果成为下一次迭代运算的 R_1，而 R_0 成为下一次迭代运算的 L_1，迭代函数 F 的功能通过多次替代和置换运算实现。第n 次迭代运算后产生的结果 L_n 和 R_n 分别成为构成密文的 R_{n+1} 和 L_{n+1}。解密运算是图 3.5 所示运算过程的逆过程，从构成密文的 R_{n+1} 和 L_{n+1} 导出 L_n 和 R_n，L_n 和 K_n 作为迭代函数 F 的输入，迭代函数 F 的输出和 R_n 进行异或运算，结果作为下一次迭代运算的 L_{n-1}，L_n 作为下一次迭代运算的 R_{n-1}。

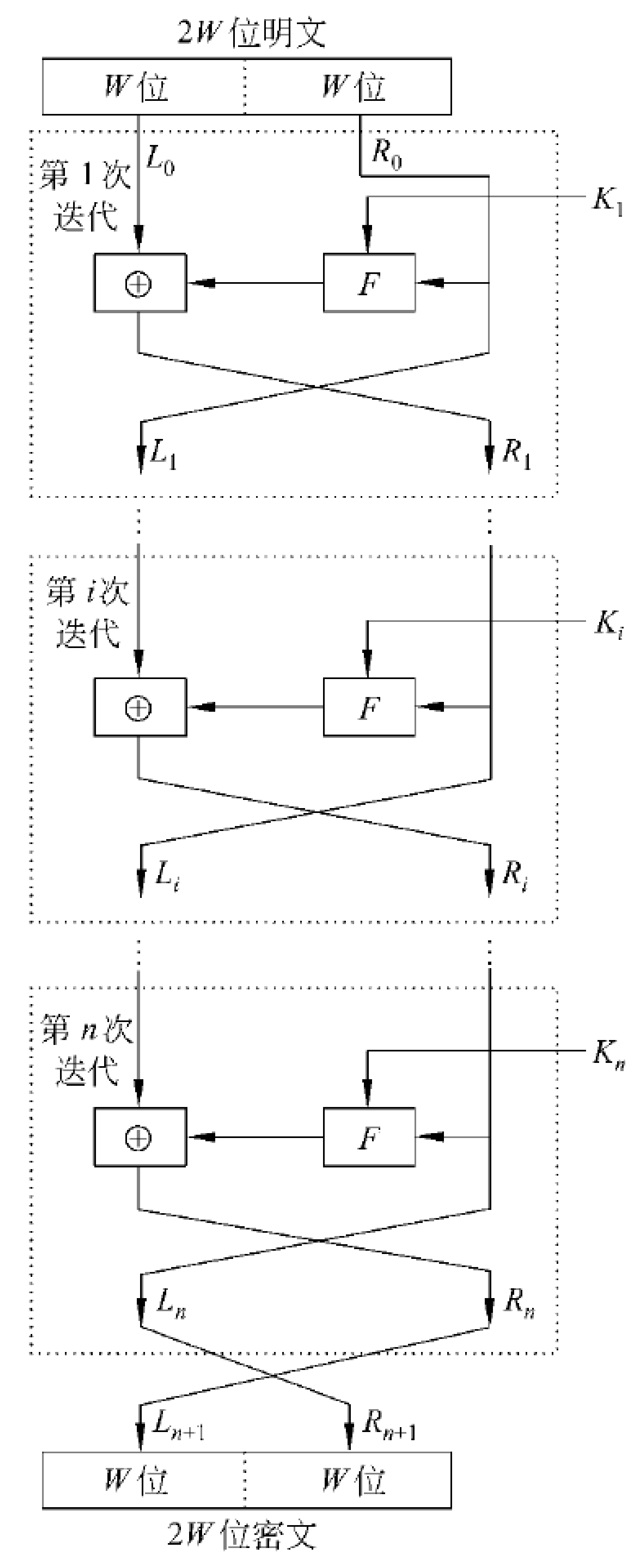


图 3.5　Feistel 分组密码结构

图 3.5 所示的分组密码加密运算过程的安全性取决于以下几个因素。

- 数据组长度：增加数据组的长度，有利于提高加密算法的安全性（不容易通过明文、密文对解析出密钥），但增加运算复杂性。
- 密钥长度：增加密钥的长度，有利于提高加密算法的安全性，但增加运算复杂性。
- 迭代次数：增加迭代次数，有利于提高加密算法的安全性，但增加运算复杂性。目前选择 16 次迭代次数就是综合考虑加密算法安全性和运算复杂性的结果。
- 子密钥序列生成算法：采用复杂的子密钥序列生成算法，有利于提高加密算法的安全性。
- 迭代函数：采用复杂的迭代函数，有利于提高加密算法的安全性。目前采用的迭代函数由多级替代和置换运算实现。

3. 对称密钥加密算法举例

1）数据加密标准

数据加密标准（Data Encryption Standard，DES）采用图 3.5 所示的分组密码结构，明文被分割成固定 64 位长度的数据组 X，数据组 X 在开始图 3.5 所示的迭代运算前，先进行初始置换运算（IP），即 $IP(X)=(L_0, R_0)$。加密运算过程中：

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$$

解密运算是加密运算的逆过程。

$$R_{i-1} = L_i$$
$$L_{i-1} = R_i \oplus F(R_{i-1}, K_i) = R_i \oplus F(L_i, K_i)$$

迭代函数的运算过程如图 3.6 所示，首先通过一个扩展函数 E 将右半部分(R_{i-1})32 位二进制数扩展为 48 位二进制数，由于 48 位二进制数是由 32 位二进制数扩展后产生的，因此，它的编码数量不是 2^{48}，而是 2^{32}，这样的编码集可以由 32 位二进制数的编码进行替代。将 32 位右半部分(R_{i-1})扩展为 48 位的目的是为了和 48 位的子密钥 K_i 进行异或运算。和子密钥异或运算后产生的 48 位结果被分成 8 组，每组 6 位，每一组结果单独进行一次替代运算 S_i，用 4 位编码替代每组 6 位结果。这里能够用 4 位编码替代 6 位结果的原因是 48 位的结果只组成 2^{32} 个编码的编码集。对 8 组 6 位结果进行替代运算后产生 8 组 4 位结果，并由它们构成 32 位的数据组，对这 32 位数据组根据置换规则 P 进行置换运算，最终产生迭代运算结果 $F(R_{i-1}, K_i)$。

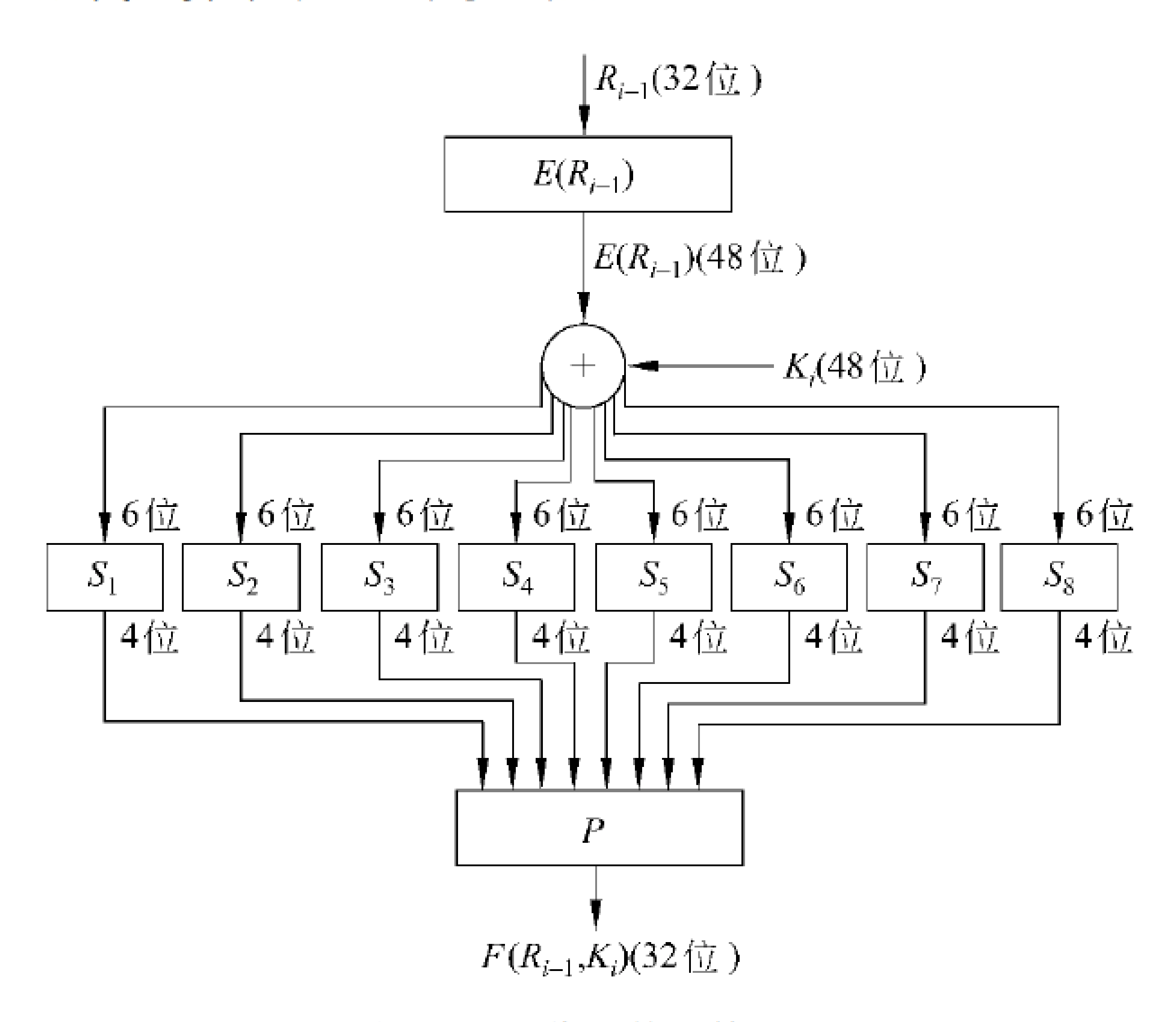


图 3.6　迭代函数运算过程

参与每一次迭代运算的子密钥是不同的，它由密钥 K 和子密钥生成算法产生。由密钥 K 产生子密钥序列的运算过程如图 3.7 所示。64 位密钥由 8 字节组成，每一个字节中，只有 7 位是密钥，另 1 位是其他 7 位的奇偶校验位，因此，64 位密钥 K 中真正作为密钥的只有 56 位，提取操作所完成的功能就是从 64 位密钥 K 中提取出真正用作密钥的 56 位二进制数。56 位密钥根据置换规则 P_1 进行置换运算，得到的结果被分成左右两部分，每部分 28 位，这两部分结果分别左移 n_1 位。产生不同的子密钥时，左移的位数不同，分别由 $n_1, n_2, \cdots, n_{16}$ 表示。如图 3.7 所示，左移后的结果作为计算下一个子密钥时的左移寄存器的输入。从左移后得到的 56 位结果中提取 48 位，对提取出的 48 位根据置换规

则 P_2 进行置换运算，置换运算结果就是本次的子密钥 K_i。

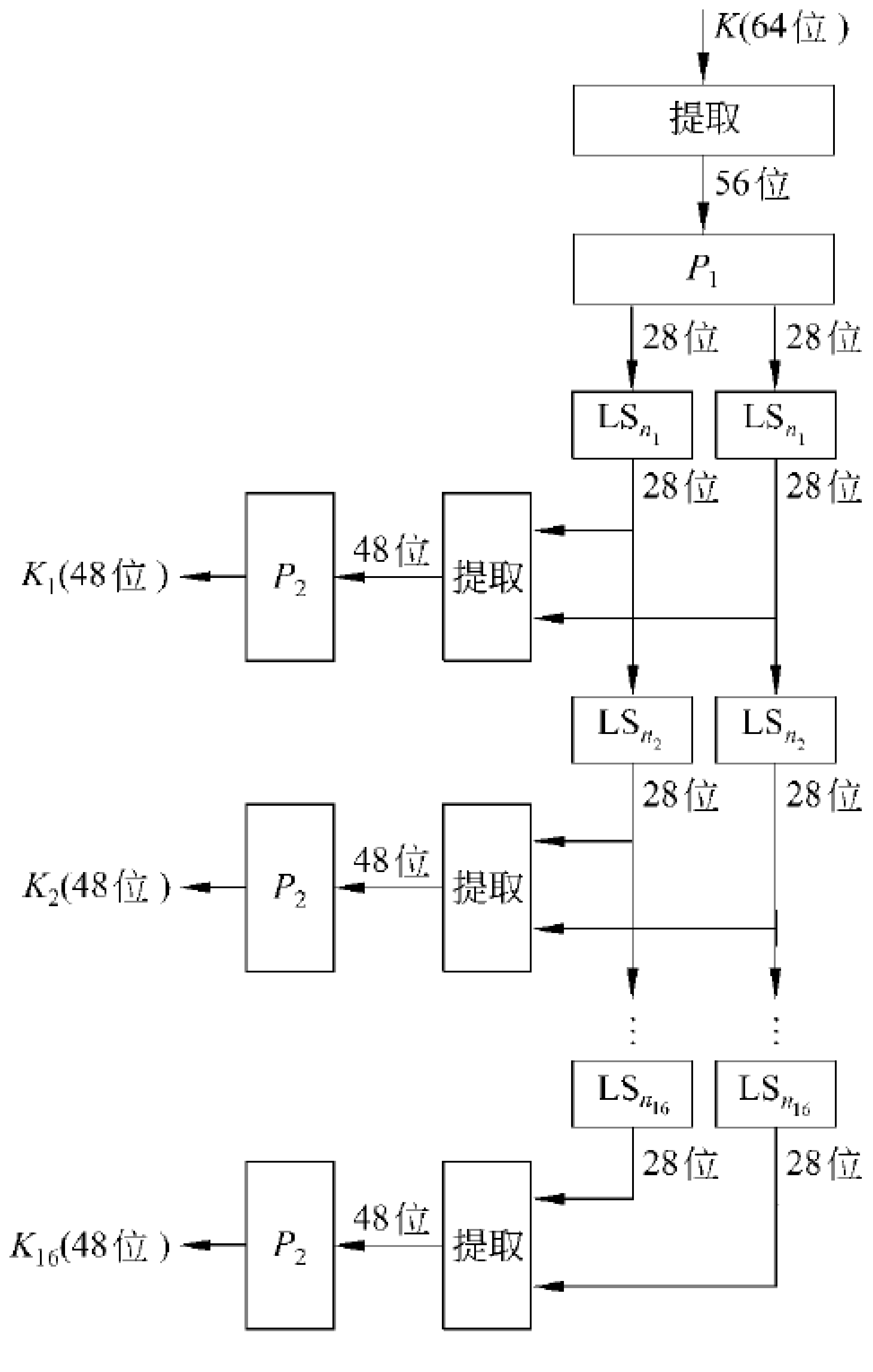


图 3.7 子密钥序列生成过程

由于 56 位长度的密钥只能产生 2^{56} 个不同的密钥，因此，在目前由高性能计算机进行密钥破解的情况下，即使采用穷举法这样简单、传统的密钥破解方法，可以在几个小时内根据密文和明文对推导出密钥 K，因此，采用 56 位密钥的 DES 加密算法并不是一种安全的对称密钥加密算法，目前实际采用的 DES 加密算法是三重 DES，加密解密过程如图 3.8 所示，密文 $Y=E_{K_3}(D_{K_2}(E_{K_1}(P)))$，明文 $P=D_{K_1}(E_{K_2}(D_{K_3}(Y)))=D_{K_1}(E_{K_2}(D_{K_3}(E_{K_3}(D_{K_2}(E_{K_1}(P))))))=D_{K_1}(E_{K_2}(D_{K_2}(E_{K_1}(P))))=D_{K_1}(E_{K_1}(P))=P$。这种加密过程相当于采用了3×56 位密钥的 DES 加密算法。对于安全性要求不是特别高的应用环境，可以采用两组 56 位密钥的三重 DES 加密算法，这种情况下，图 3.8 的密钥 K_3 由密钥 K_1 代替。

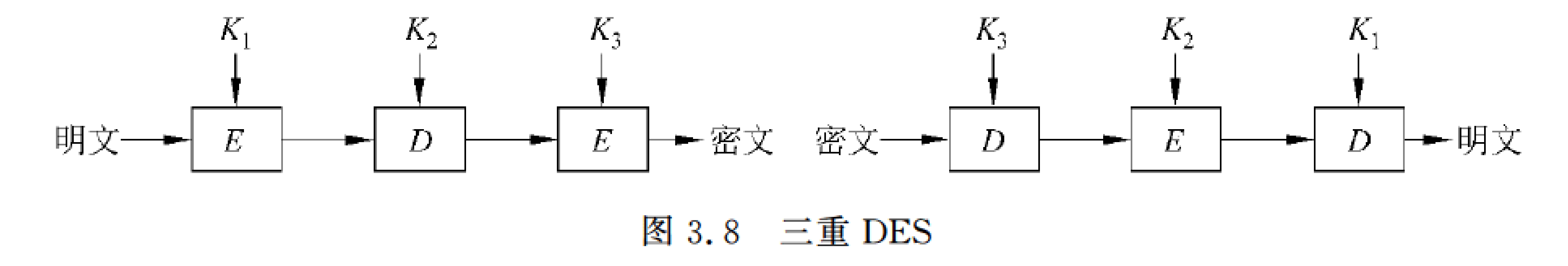


图 3.8 三重 DES

2）高级加密标准

高级加密标准（Advanced Encryption Standard，AES）将明文分割成固定 128 位长度

的数据组，密钥可以是 128 位、192 位或者 256 位（这里只讨论 128 位密钥的情况），和 DES 不同，AES 不再将数据组分成等长的两部分，而是以 128 位为单位进行迭代运算，整个加密运算过程如图 3.9 所示。128 位密钥经过扩展运算成为 11×128 位，构成子密钥序列{K_0，K_1，…，K_{10}}，每一个子密钥和数据组长度相同，为 128 位。AES 中子密钥序列由一组 32 位的字组成，$W[i]$，$0 \leqslant i \leqslant 43$，在这一组字中，子密钥 K_0 对应的 4 个字为 $W[i]$（$0 \leqslant i \leqslant 3$），以此类推，子密钥 K_j 对应的 4 个字为字 $W[i]$（$j \times 4 \leqslant i \leqslant j \times 4+3$）。在开始第 1 次迭代运算前，数据组先和子密钥 K_0 进行异或运算，运算结果作为第 1 次迭代运算的输入。除第 10 次迭代运算外，每一次迭代运算过程包括逐字节替代运算、逐行置换运算、逐列变换运算和与子密钥 K_i 的异或运算。为了实现这些运算，128 位的数据组被分成 16 字节，16 字节又被组织成 4×4 的矩阵，如图 3.10 所示，A_i 是构成 128 位数据组中的某个字节，$S_{r,c}$ 是对应的 A_i 在矩阵中的表示，其中，r 是行号，c 是列号。构成子密钥 K_i 的每一个字对应矩阵中的一列，4 个字对应矩阵中的 4 列。

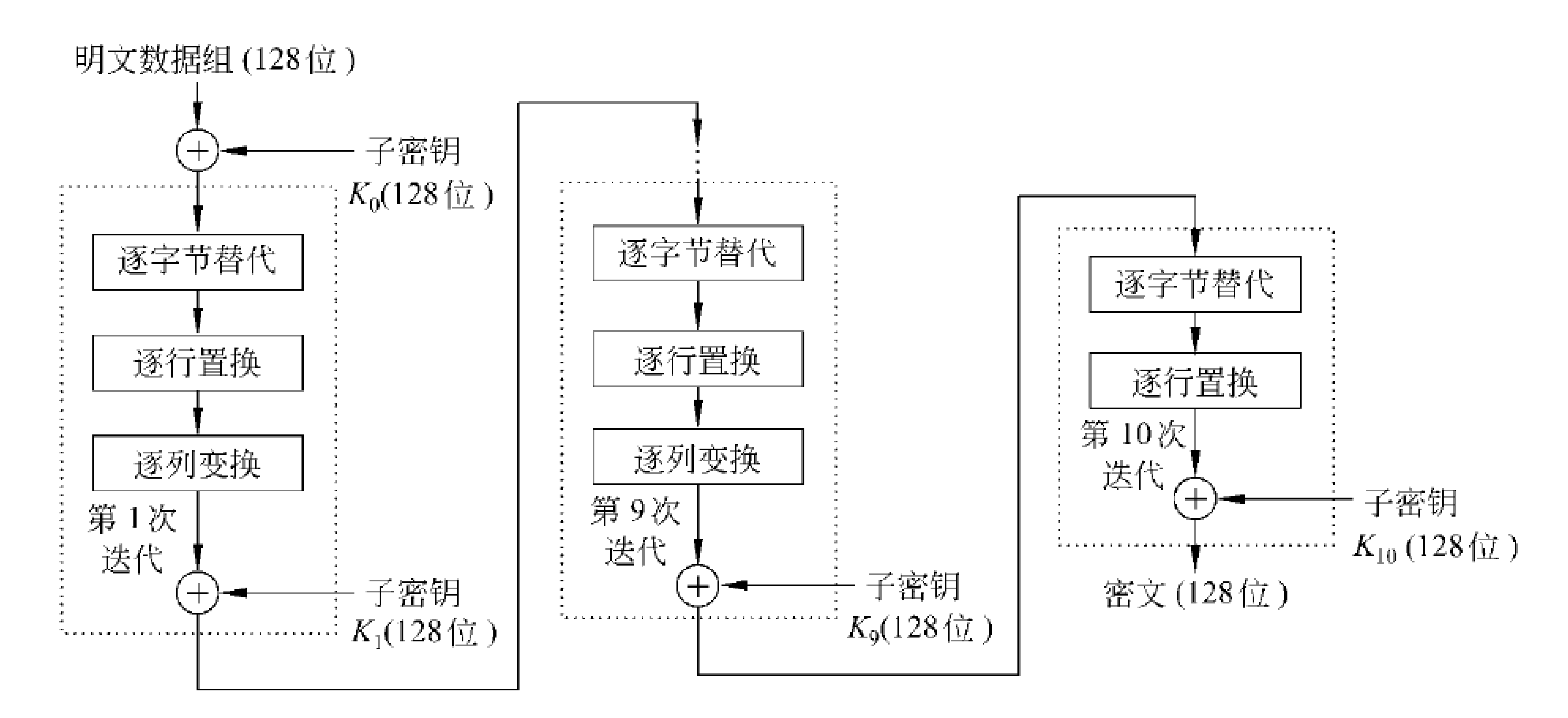


图 3.9　AES 加密运算过程

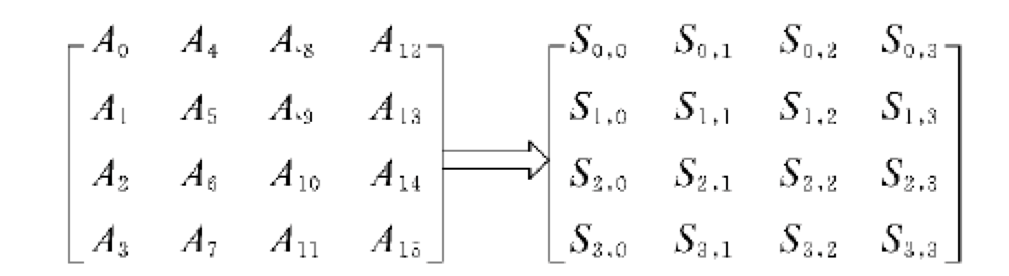


图 3.10　矩阵表示的 128 位数据组

逐字节替代运算是指矩阵中每一个字节独立进行替代运算，矩阵中每一个字节以该字节值为索引，检索替代表，找到对应的 8 位替代值予以替代，如原值 00H 用 63H 替代，原值 FFH 用 16H 替代。

逐行置换运算过程如图 3.11 所示，置换规则是：$S'_{r,c}=S_{r,c+\mathrm{shift}(r) \bmod 4}$，其中 shift(0)=0，shift(1)=1，shift(2)=2，shift(3)=3，因此，

$$\begin{bmatrix} S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ S_{1,0} & S_{1,1} & S_{1,2} & S_{1,3} \\ S_{2,0} & S_{2,1} & S_{2,2} & S_{2,3} \\ S_{3,0} & S_{3,1} & S_{3,2} & S_{3,3} \end{bmatrix} \xrightarrow{\text{逐行置换运算}} \begin{bmatrix} S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ S_{1,1} & S_{1,2} & S_{1,3} & S_{1,0} \\ S_{2,2} & S_{2,3} & S_{2,0} & S_{2,1} \\ S_{3,3} & S_{3,0} & S_{3,1} & S_{3,2} \end{bmatrix} = \begin{bmatrix} S'_{0,0} & S'_{0,1} & S'_{0,2} & S'_{0,3} \\ S'_{1,0} & S'_{1,1} & S'_{1,2} & S'_{1,3} \\ S'_{2,0} & S'_{2,1} & S'_{2,2} & S'_{2,3} \\ S'_{3,0} & S'_{3,1} & S'_{3,2} & S'_{3,3} \end{bmatrix}$$

图 3.11 逐行置换运算过程

$$S'_{0,c} = S_{0,c}$$
$$S'_{1,c} = S_{0,c+1 \bmod 4}$$
$$S'_{2,c} = S_{0,c+2 \bmod 4}$$
$$S'_{3,c} = S_{0,c+3 \bmod 4}$$

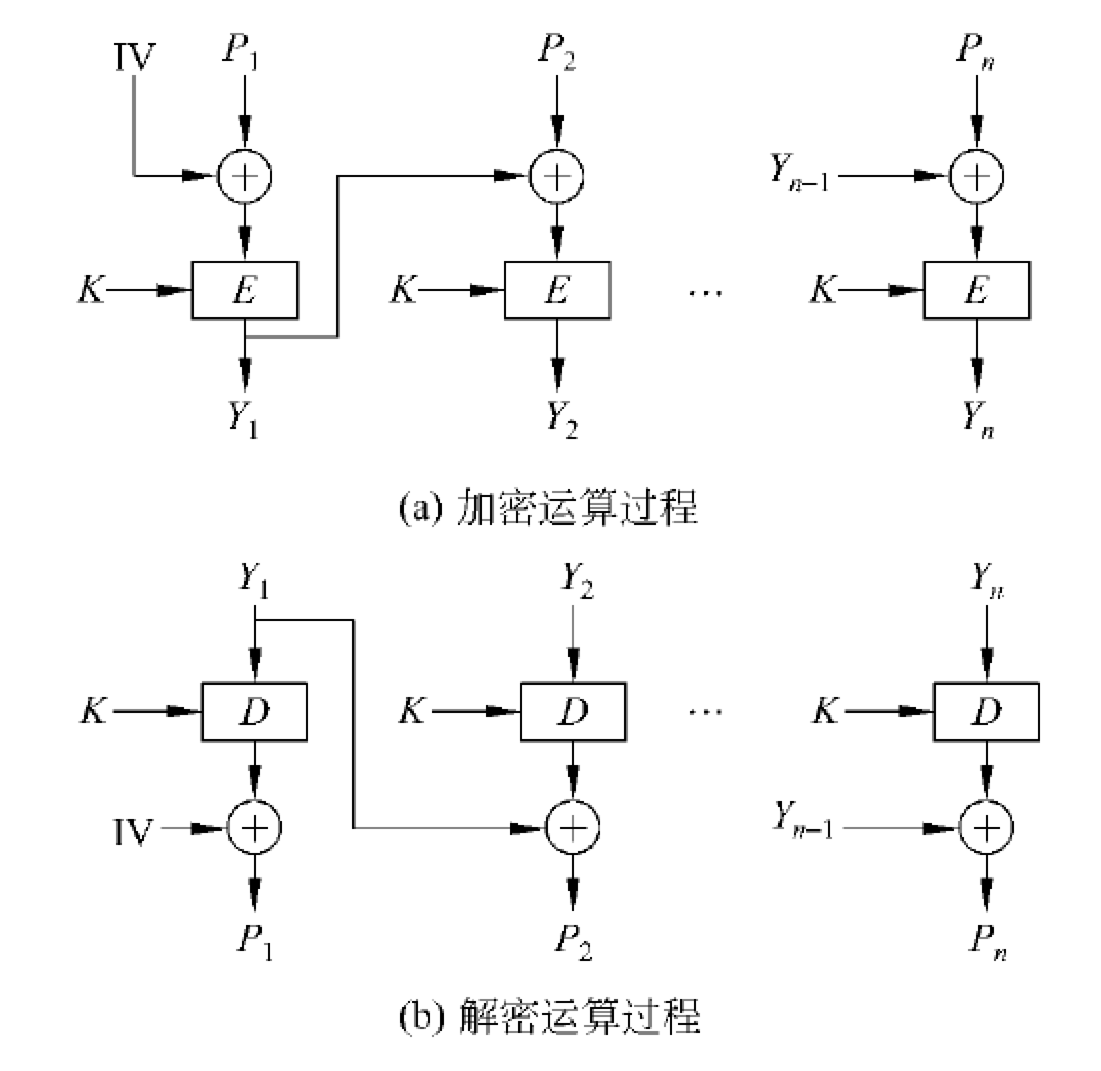
逐列变换运算过程如图 3.12 所示。

$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix}$$

图 3.12 逐列变换运算过程

3）加密分组链接

分组密码体制对由明文分割产生的数据组独立进行加密运算，如果两组数据组相同，且这两组数据组加密运算时使用的密钥也相同，这两组数据组将生成相同的密文。对于对称密钥加密算法，很难对不同的数据组使用不同的密钥，因此，当明文有规则重复时，加密后的密文也同样有规则重复，这样有利于破解密文，降低加密算法的安全性，为了避免发生相同数据组加密后产生相同密文的情况，采用图 3.13 所示的加密分组链接（Cipher-Block Chaining，CBC）的方法。



(a) 加密运算过程

(b) 解密运算过程

图 3.13 加密分组链接模式

在图 3.13 所示的加密分组链接模式中，加密运算模块的输入不是分割明文后产生的数据组 P_i，而是数据组 P_i 和前一次加密运算后的结果 Y_{i-1} 异或运算后的结果。

$$Y_i = E_K(Y_{i-1} \oplus P_i)$$

第 1 组数据组和初始向量 IV 的异或运算结果作为加密运算模块的输入。

$$Y_1 = E_K(\mathrm{IV} \oplus P_1)$$

在接收端，为了还原数据组 P_i，必须进行以下运算过程。

$$D_K(Y_i) = D_K(E_K(Y_{i-1} \oplus P_i)) = Y_{i-1} \oplus P_i$$

$$Y_{i-1} \oplus D_K(Y_i) = Y_{i-1} \oplus Y_{i-1} \oplus P_i = P_i$$

因此，数据组 P_i 是对应密文 Y_i 解密运算后的结果和前一组数据组对应密文异或运算后的结果。同样，

$$P_1 = \mathrm{IV} \oplus D_K(Y_1)$$

因此，发送端和接收端必须具有相同的初始向量 IV。

由于加密分组链接模式中每一组数据组和前一组数据组对应的密文异或运算后作为加密运算模块的输入，因此，即使密钥相同，两组相同数据组加密运算后产生的密文也不会相同，增加了加密算法的安全性，因此，加密分组链接模式在分组密码体制中得到了广泛应用。

4. 对称密钥加密算法的密钥分配过程

由于加密、解密算法是标准的、公开的，安全性就完全基于密钥的保护上。由于通信双方都需要拥有共同的密钥，而且，如果长期使用同一密钥的话，泄露密钥的可能性就会增加，因此，如何分配密钥就成了一大难题。可靠的办法是让信使携带密封的密钥给互相通信的各个用户，但在网络如此发达的今天，仍然采用这种笨方法有点不合时宜，而且，如果经常变换通信对象，为了安全，也定期更换密钥的话，这种方法也很难操作。因此，需要采用通过网络分配密钥的方法。

目前常用的通过网络分配密钥的方法是建立一个密钥分配中心（Key Distribution Center，KDC），由 KDC 负责为用户分配密钥。需要 KDC 分配密钥的用户先注册到 KDC，获得和 KDC 通信时使用的密钥。当某个注册用户 A 希望和另一个注册用户 B 用密文通信时，通过向 KDC 申请，获得这一次通信所使用的密钥，如图 3.14 所示。

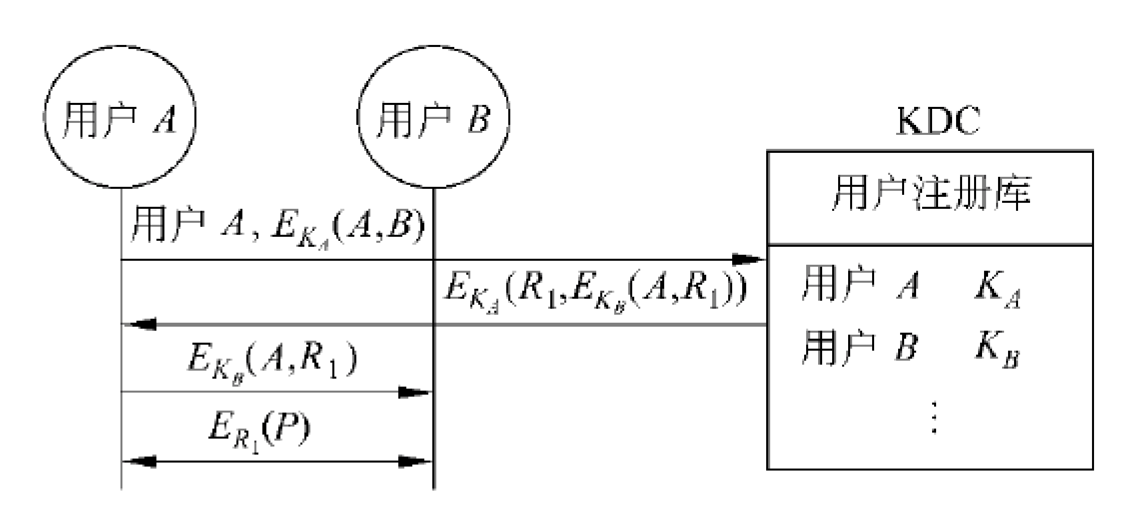


图 3.14　密钥分配过程

（1）用户 A 将希望和用户 B 通信的请求用 KDC 分配给自己的密钥 K_A 进行加密，然后将加密后的请求：$E_{K_A}(A,B)$和自己的用户名一起发送给 KDC。

（2）KDC 用随机数生成算法产生一个密钥 R_1 供用户 A 和用户 B 通信时使用，这种

密钥只用于这一次通信,称之为"一次一密"。KDC将密钥R_1用分配给用户A的密钥加密后发送给用户A,除了密钥R_1,KDC还将用分配给用户B的密钥K_B加密用户A希望和用户B通信的请求及密钥R_1,并将加密后的内容包含在用K_A加密的数据中。因此,当用户A用KDC分配给它的密钥K_A解密KDC发送给它的密文后,得到由KDC生成并分配给这一次用户A和用户B通信时使用的密钥R_1,同时得到用KDC分配给用户B的密钥加密的用户A希望和用户B通信的请求及密钥R_1。由于是用分配给用户B的密钥加密的密文,用户A无法解密,向用户B转发该密文。

(3) 用户B用KDC分配给它的密钥K_B解密该密文,获知用户A希望和它通信并使用KDC分配的一次性密钥R_1,双方用R_1作为密钥,对相互传输的数据进行加密、解密操作。

为了提高安全性,KDC分配给注册用户的密钥如K_A、K_B也需要经常更换。

3.1.2 公开密钥加密算法

1. 公开密钥加密算法原理

公开密钥加密算法使用不同的加密密钥和解密密钥,它的加密、解密过程如图3.15所示,发送者用加密算法E和密钥P_K对明文P进行加密,接收者用解密算法D和密钥S_K对密文Y进行解密。加密密钥P_K是公开的,而解密密钥S_K是保密的,只有接收者知道,用于解密用公开密钥加密的密文,习惯上将加密密钥称为公钥,而将解密密钥称为私钥。

$$Y=E_{P_K}(P)$$

$$D_{S_K}(Y)=D_{S_K}(E_{P_K}(P))=P$$

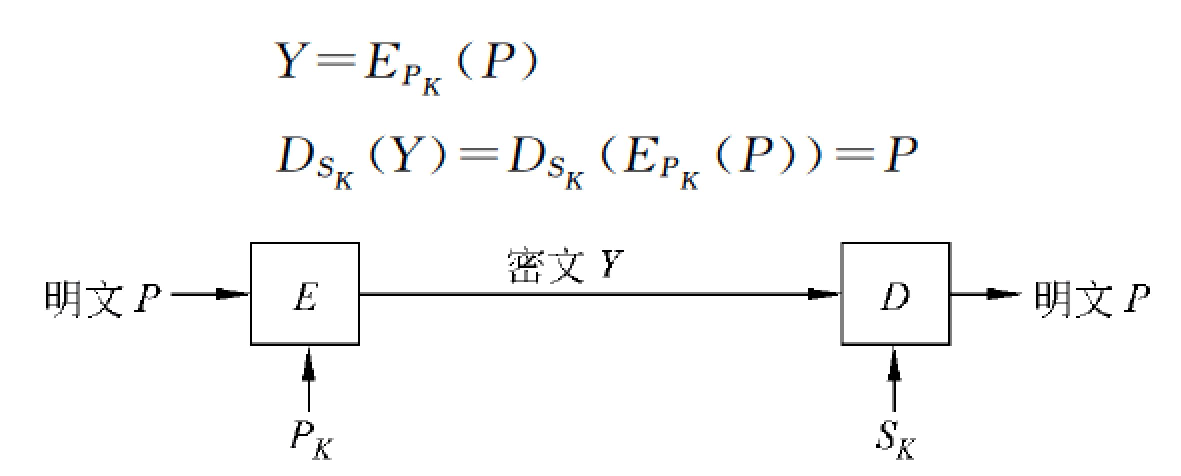


图3.15 公开密钥加密算法的加密、解密过程

公开密钥加密算法的原则是:

(1) 容易成对生成密钥P_K和S_K。

(2) 加密和解密算法是公开的,而且可以对调:

$$D_{S_K}(E_{P_K}(P))=E_{P_K}(D_{S_K}(P))=P$$

(3) 加密和解密过程容易实现。

(4) 从计算可行性讲,无法根据P_K推导出S_K。

(5) 从计算可行性讲,无法根据P_K和密文Y推导出明文P。

2. 公开密钥加密算法举例

目前使用最广泛的公开密钥加密算法是RSA和Diffie-Hellman公开密钥加密算法。

1) RSA公开密钥加密算法

RSA(Rivest-Shamir-Adleman)公开密钥加密算法也是一种分组密码算法,每一组数

据是 0～$n-1$ 的整数，n 和密钥的长度相关。

$$Y=P^e \bmod n$$
$$P=Y^d \bmod n=(P^e)^d \bmod n=P^{ed} \bmod n$$

发送者和接收者都需知道整数对(e,n)，但只有接收者知道整数 d，因此，公开密钥(简称公钥)$P_K=(e,n)$，秘密密钥(简称私钥)$S_K=(d,n)$。实现 RSA 公开密钥加密算法的前提是：

(1) 能够找到整数 e、d 和 n，对所有 0～$n-1$ 的整数 P，满足等式 $P=P^{ed} \bmod n$。

(2) 对所有 0～$n-1$ 的整数 P，计算 P^e 和 Y^d 是可行的。

(3) 从计算可行性讲，无法根据 e 和 n，推导出 d。

RSA 公开密钥加密算法的基本思想是：根据数论，寻求两个大素数比较简单，但将它们的乘积分解开则极其困难。根据上述思想求出 e、d 和 n 的过程如下：

① 选择两个不同的大素数 p 和 q，使得 $n=p\times q$。

② 计算欧拉函数 $\Phi(n)=(p-1)\times(q-1)$。

③ 从 0～$\Phi(n)-1$ 中选择一个与 $\Phi(n)$互素的数作为 e。

④ 求出满足等式 $ed=1 \bmod \Phi(n)$的 d。

当 n 足够大时，很难通过 e 推导出 d。下面通过一个实例来说明 RSA 公开密钥加密算法的加密、解密过程。

求出 n、e 和 d 的过程如下，公钥 $P_K=(n,e)$，私钥 $S_K=(n,d)$。

① 选择两个不同的素数 $p=17$，$q=11$。

② 求出 $n=p\times q=17\times 11=187$。

③ 求出欧拉函数 $\Phi(n)=(p-1)\times(q-1)=16\times 10=160$。

④ 选择 $e=7$。

⑤ 根据 $7\times d=1 \bmod 160$，求出 $d=23$，($7\times 23=161$，$161 \bmod 160=1$)。

假定分割明文后产生的某一组数据组是 88($P=88$)。

加密过程如下：

对应密文 $Y=P^e \bmod n=88^7 \bmod 187=11$。

解密过程如下：

密文 11 对应的明文 $P=Y^d \bmod n=11^{23} \bmod 187=88$。

很显然，RSA 私钥的安全性取决于 n 的长度，当 n 为 1024 位二进制数时，根据目前的计算能力，RSA 私钥的安全性是可以保证的。但 n 长度越大，加密和解密运算的计算复杂度越高。

2) Diffie-Hellman 密钥交换算法

根据公开密钥加密算法的定义，Diffie-Hellman 密钥交换算法并不是一种真正意义上的公开密钥加密算法，它本身不能直接用于加密、解密数据，但它可以根据公开密钥和秘密密钥的思路实现发送者和接收者之间的密钥交换过程。

对于选定的大素数 p，如果集合$\{\alpha \bmod p, \alpha^2 \bmod p, \cdots, \alpha^{p-1} \bmod p\}$包含了 1～$p-1$ 的所有整数，则称 α 是素数 p 的原根。因此，对于 1～$p-1$ 的任何整数 b，存在下列等式。

$$b=\alpha^i \bmod p,\quad 1\leqslant i\leqslant p-1$$

这里的 i 是唯一的，称为 b 以 α 为基模 p 的指数，或者称为 b 以 α 为基模 p 的离散对数，记作 $\mathrm{ind}_{\alpha,p}(b)$。

Diffie-Hellman 密钥交换算法的前提是选择一个大素数 p 和它对应的原根 α，如果用户 A 希望和用户 B 交换密钥 K，则分别作如下计算：

(1) 用户 A 选择一个小于 p 的随机整数 X_A，使得 $Y_A=\alpha^{X_A} \bmod p$，将 X_A 作为私钥，将 Y_A 作为公钥公告给用户 B。

(2) 用户 B 选择一个小于 p 的随机整数 X_B，使得 $Y_B=\alpha^{X_B} \bmod p$，将 X_B 作为私钥，将 Y_B 作为公钥公告给用户 A。

(3) 用户 A 根据自身的私钥 X_A 和用户 B 公告的公钥 Y_B，求出密钥 $K_A=Y_B^{X_A} \bmod p$。

(4) 用户 B 根据自身的私钥 X_B 和用户 A 公告的公钥 Y_A，求出密钥 $K_B=Y_A^{X_B} \bmod p$。

(5) 双方求出的密钥相同，$K_A=K_B=K$。

下面通过一个实例讨论一下 Diffie-Hellman 密钥交换算法实现双方密钥同步的过程。

① 选择素数 $p=71$，原根 $\alpha=7$。

② 用户 A 选择 $X_A=5$，求出 $Y_A=\alpha^{X_A} \bmod p=7^5 \bmod 71=51$。

③ 用户 B 选择 $X_B=12$，求出 $Y_B=\alpha^{X_B} \bmod p=7^{12} \bmod 71=4$。

④ 用户 A 求出 $K_A=Y_B^{X_A} \bmod p=4^5 \bmod 71=30$。

⑤ 用户 B 求出 $K_B=Y_A^{X_B} \bmod p=51^{12} \bmod 71=30$。

⑥ $K_A=K_B=K=30$。

图 3.16 是用户 A 和用户 B 用 Diffie-Hellman 密钥交换算法同步密钥 K 的过程。

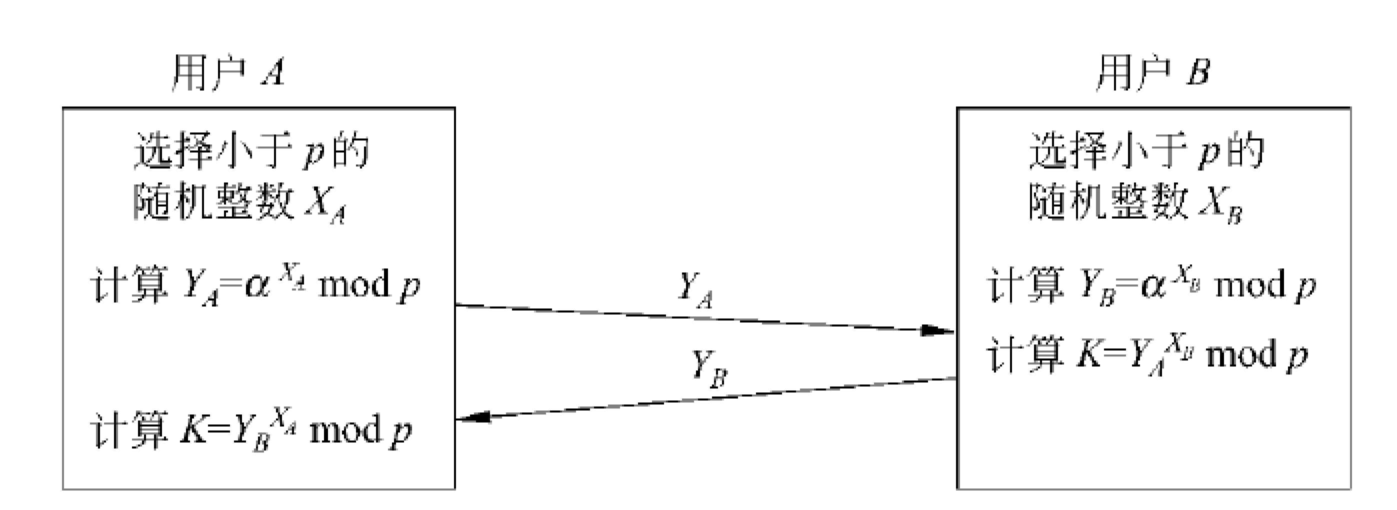


图 3.16 Diffie-Hellman 密钥交换算法同步密钥 K 的过程

同样，Diffie-Hellman 私钥的安全性取决于大素数 p 的长度，大素数 p 的长度越大，私钥安全性越好，但计算密钥的过程越复杂，目前定义了三组不同长度的大素数 p 和对应的原根 α。

第 1 组　大素数 p 是 768 位二进制数。

第 2 组　大素数 p 是 1024 位二进制数。

第 3 组　大素数 p 是 1536 位二进制数。

在使用 Diffie-Hellman 密钥交换算法时，只要选择参数组号，就可确定所使用的大素数 p 和对应的原根 α，上述三组参数分别称谓 D-H-1 组、D-H-2 组和 D-H-3 组

3.2 报文摘要算法

3.2.1 报文摘要算法要求

报文摘要算法的目的就是产生用来标识某个任意长度报文的有限位数信息，即报文摘要，而且这种标识信息就像报文的指纹一样，具有确认性和唯一性。假定 MD 为报文摘要算法，MD(X)是算法对报文 X 作用后产生的标识信息，MD 必须满足如下要求：

- 能够作用于任意长度的报文；
- 产生有限位数的标识信息；
- 易于实现；
- 具有单向性，即只能根据报文 X 求出 MD(X)，从计算可行性讲，无法根据标识信息 h，得出报文 X，且使得 MD(X)$=h$；
- 从计算可行性讲，对于任何报文 X，无法找出另一个报文 Y，$X \neq Y$，但 MD(X)$=$MD(Y)。
- 即使只改变报文 X 中一位二进制位，也使得重新计算后的 MD(X)变化很大。

3.2.2 MD5

报文摘要第 5 版（Message Digest，Version 5，MD5）是较早推出的报文摘要算法，它将任意长度的报文转变为 128 位的报文摘要，即假定 P 为任意长度的报文，$h=$MD5(P)，则 h 的长度为 128 位。MD5 的运算过程如下。

1. 添加填充位

假定报文的长度为 X，首先添加首位为 1，其余位为 0 的填充位，填充位的长度 Y 由下式确定。

$$(X+Y) \bmod 512=448$$

由于填充位是不可缺少的，因此，填充位的长度 Y 在 1～512 之间。填充位后面是 64 位的报文长度，由于报文长度 X 是任意的，当报文长度无法用 64 位二进制数表示时，取报文长度的最低 64 位。添加填充位和报文长度后的数据序列如图 3.17 所示，它的长度是 512 位的整数倍。

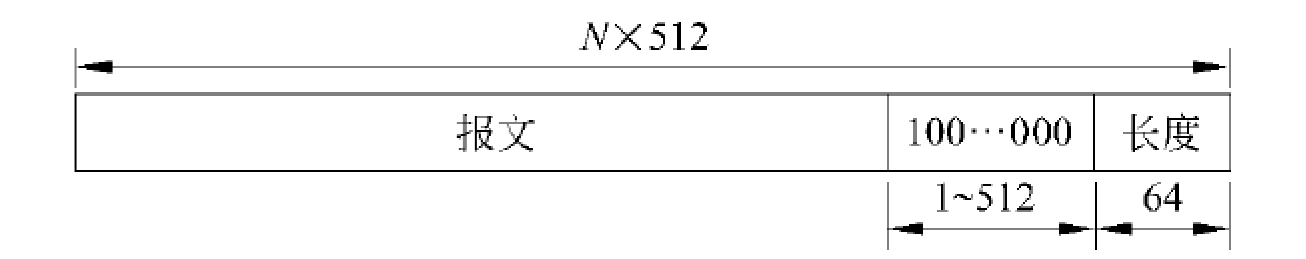


图 3.17 添加操作后的数据序列

2. 分组操作

MD5 将添加填充位和报文长度的数据序列分割成长度为 512 位的数据组，每一组数据组单独进行报文摘要运算，报文摘要运算的输入是 512 位的数据组和前一组数据组进行报文摘要运算后的 128 位结果，第一组数据组进行报文摘要运算时，需要输入第一组数

据组和初始向量 IV，初始向量 IV 和中间结果分为 4 个 32 位的字，它们分别称为 A、B、C 和 D（见图 3.18）。这 4 个字作为初始向量时的初值如下：

$$A=67452301\text{H}$$
$$B=\text{EFCDAB89H}$$
$$C=\text{98BADCFEH}$$
$$D=10325476\text{H}$$

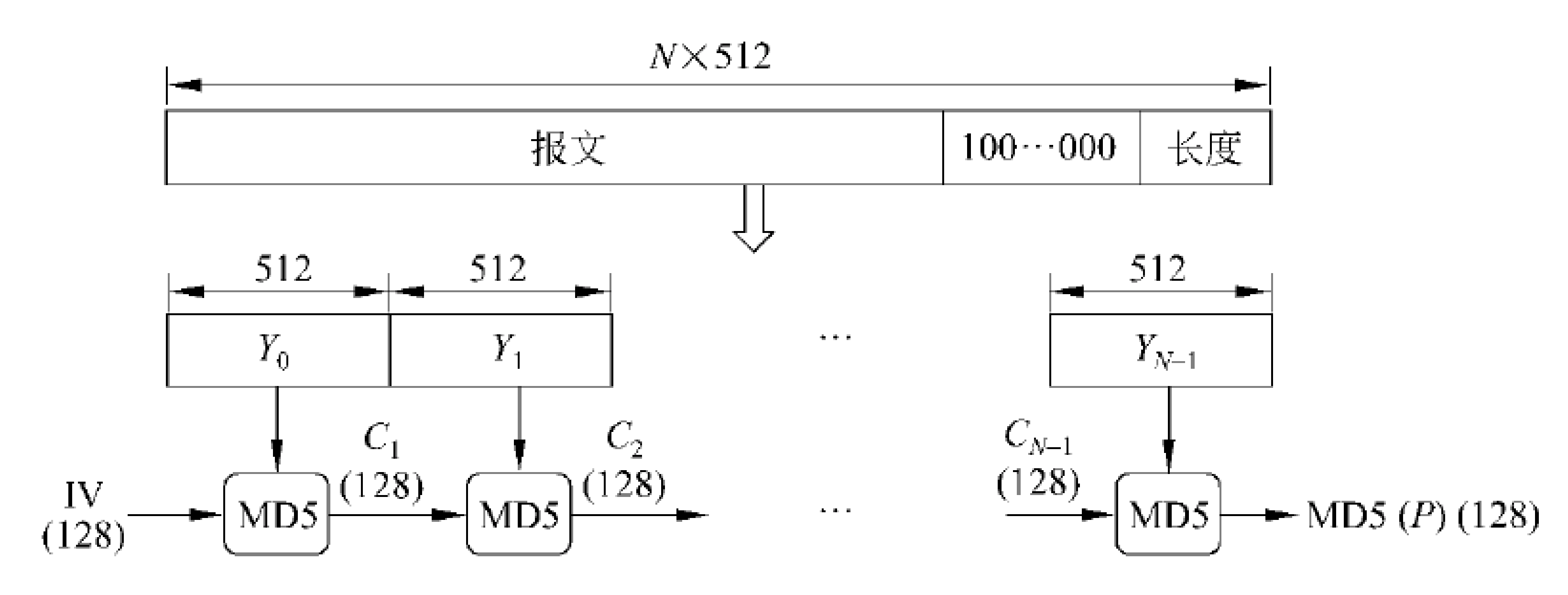


图 3.18　分组操作过程

3. MD5 运算过程

MD5 运算过程包含 4 级运算（见图 3.19 和表 3.1），每一级运算单独定义了函数，4 级运算对应的函数如下。

$F(X,Y,Z)=X\cdot Y+/X\cdot Z$（$/X$ 表示对 X 非操作）

$G(X,Y,Z)=X\cdot Z+Y\cdot /Z$

$H(X,Y,Z)=X\oplus Y\oplus Z$

$I(X,Y,Z)=Y\oplus(X+/Z)$

这 4 个函数的输入是 3 个 32 位的字，输出是 1 个32 位的字。每一级运算过程的输入是 512 位的数据组和上一级运算的结果，输出是 4 个 32 位的字。第一级运算过程输入的 4 个 32 位的字是对前一组数据组进行 MD5 运算得到的结果。512 位数据组被分成 16 个 32 位的字，分别是 $M[k]$，$0\leqslant k\leqslant 15$。同时 MD5 也产生 64 个 32 位的常数，分别是 $T[i]$，$1\leqslant i\leqslant 64$。每一级运算过程进行 16 次运算，每一次运算都有构成数据组的其中一个字和其中一个常数参加，构成数据组的 16 字参加每一级的 16 次运算，但参加每一级 16 次运算的常数是不同的，参加第 i 级 16 次运算的常数是 $T[j]$（$(i-1)\times 16\leqslant j\leqslant (i-1)\times 16+15$）。每一级运算的公式如下：

图 3.19　MD5 运算过程

$\text{FF}(a,b,c,d,M[k],s,i)$；$a=b+((a+F(b,c,d)+M[k]+T[i])\angle s)$

$\text{GG}(a,b,c,d,M[k],s,i)$；$a=b+((a+G(b,c,d)+M[k]+T[i])\angle s)$

$\text{HH}(a,b,c,d,M[k],s,i)$；$a=b+((a+H(b,c,d)+M[k]+T[i])\angle s)$

表 3.1　MD5 运算过程

第一级运算过程的 16 次函数调用			
FF(A,B,C,D,M[0],7,1)	FF(D,A,B,C,M[1],12,2)	FF(C,D,A,B,M[2],17,3)	FF(B,C,D,A,M[3],22,4)
FF(A,B,C,D,M[4],7,5)	FF(D,A,B,C,M[5],12,6)	FF(C,D,A,B,M[6],17,7)	FF(B,C,D,A,M[7],22,8)
FF(A,B,C,D,M[8],7,9)	FF(D,A,B,C,M[9],12,10)	FF(C,D,A,B,M[10],17,11)	FF(B,C,D,A,M[11],22,12)
FF(A,B,C,D,M[12],7,13)	FF(D,A,B,C,M[13],12,14)	FF(C,D,A,B,M[14],17,15)	FF(B,C,D,A,M[15],22,16)
第二级运算过程的 16 次函数调用			
GG(A,B,C,D,M[1],5,17)	GG(D,A,B,C,M[6],9,18)	GG(C,D,A,B,M[11],14,19)	GG(B,C,D,A,M[0],20,20)
GG(A,B,C,D,M[5],5,21)	GG(D,A,B,C,M[10],9,22)	GG(C,D,A,B,M[15],14,23)	GG(B,C,D,A,M[4],20,24)
GG(A,B,C,D,M[9],5,25)	GG(D,A,B,C,M[14],9,26)	GG(C,D,A,B,M[3],14,27)	GG(B,C,D,A,M[8],20,28)
GG(A,B,C,D,M[13],5,29)	GG(D,A,B,C,M[2],9,30)	GG(C,D,A,B,M[7],14,31)	GG(B,C,D,A,M[12],20,32)
第三级运算过程的 16 次函数调用			
HH(A,B,C,D,M[5],4,33)	HH(D,A,B,C,M[8],11,34)	HH(C,D,A,B,M[11],16,35)	HH(B,C,D,A,M[14],23,36)
HH(A,B,C,D,M[1],4,37)	HH(D,A,B,C,M[4],11,38)	HH(C,D,A,B,M[7],16,39)	HH(B,C,D,A,M[10],23,40)
HH(A,B,C,D,M[13],4,41)	HH(D,A,B,C,M[0],11,42)	HH(C,D,A,B,M[3],16,43)	HH(B,C,D,A,M[6],23,44)
HH(A,B,C,D,M[9],4,45)	HH(D,A,B,C,M[12],11,46)	HH(C,D,A,B,M[15],16,47)	HH(B,C,D,A,M[2],23,48)
第四级运算过程的 16 次函数调用			
II(A,B,C,D,M[0],6,49)	II(D,A,B,C,M[7],10,50)	II(C,D,A,B,M[14],15,51)	II(B,C,D,A,M[5],21,52)
II(A,B,C,D,M[12],6,53)	II(D,A,B,C,M[3],10,54)	II(C,D,A,B,M[10],15,55)	II(B,C,D,A,M[1],21,56)
II(A,B,C,D,M[8],6,57)	II(D,A,B,C,M[15],10,58)	II(C,D,A,B,M[6],15,59)	II(B,C,D,A,M[13],21,60)
II(A,B,C,D,M[4],6,61)	II(D,A,B,C,M[11],10,62)	II(C,D,A,B,M[2],15,63)	II(B,C,D,A,M[9],21,64)

$$II(a,b,c,d,M[k],s,i):a=b+((a+I(b,c,d)+M[k]+T[i])\angle s)$$

每一次运算产生一个 32 位的字,公式中的加号表示或运算,$\angle s$ 表示对运算符前面括号内的结果循环左移 s 位。公式中给出的参数是虚参,表 3.1 中给出的是每一级 16 次运算时给出的实参,以第一级为例,前面 4 次运算分别改变了作为这一级运算过程输入的 4 个 32 位字,改变的结果与数据组的内容和 MD5 选定的常数有关,每一级运算过程通过 16 次迭代使得输出的 4 个 32 位的字和数据组中的每一个字相关。

最后一级输出的 4 个 32 位字和作为这次 MD5 运算的输入的前一组数据组的 MD5 运算结果逐字相加,产生这一组数据组的 MD5 运算结果。

3.2.3 SHA-1

安全散列算法第 1 版(Secure Hash Algorithm 1,SHA-1)和 MD5 非常相似,主要不同点在于:一是初始向量 IV 和每一组数据组经过 SHA-1 运算后的结果为 5 个 32 位的字,即 160 位,而不是 128 位。这样,使得对于任何报文 X,找出另一个报文 Y,$X\neq Y$,但 $MD(X)=MD(Y)$ 的可能性更低。SHA-1 初始向量的前 4 个字的内容和 MD5 相同,第 5 个字的内容为

$$E=C3D2E1F0H$$

二是每一级的运算过程不同,SHA-1 将 16 个 32 位字的数据组 $M[k](0\leqslant k\leqslant 15)$,扩展为 80 个 32 位的字 $W[i](0\leqslant i\leqslant 79)$。每一级运算使用的函数如下:

$$F_1(X,Y,Z)=X\cdot Y+/X\cdot Z$$

$$F_2(X,Y,Z)=X\oplus Y\oplus Z$$

$$F_3(X,Y,Z)=X\cdot Y+X\cdot Z+Y\cdot Z$$

$$F_4(X,Y,Z)=X\oplus Y\oplus Z$$

完成每一级运算过程需要 20 次迭代运算,第 i 级运算进行的 20 次迭代运算如下:

```
FOR j=(i-1)×20 to(i-1)×20+19
{
    TEMP=S^5(A)+F_i(B,C,D)+E+W[j]+K_i;
    E=D;D=C;C=S^30(B);B=A;A=TEMP;
}
```

$S^5(A)$表示对字 A 循环左移 5 位。

每一级运算时使用的常数 K_i 如下:

$$K_1=5A827999H$$

$$K_2=6ED9EBA1H$$

$$K_3=8F1BBCDCH$$

$$K_4=CA62C1D6H$$

3.2.4 HMAC

报文摘要运算的主要用途是对报文进行完整性检测和报文发送者身份认证,但由于报文摘要算法的公开性,获得报文,即可计算出对应的报文摘要,因此,必须将报文摘要算

法和加密算法相结合才能实现报文的完整性检测和发送者身份认证。图3.20给出了报文完整性检测和发送者身份认证的过程。发送端对根据明文计算出的报文摘要进行加密,并附在明文后一起发送给接收端。接收端接收到明文和附在明文后面的对报文摘要加密生成的密文后,先对密文解密得到发送者计算出的报文摘要,然后对接收到的明文进行报文摘要运算,并将计算结果和解密后的报文摘要进行比较,如果相等,表示信息在传输过程中未被篡改,如果不相等,则表示信息已经被篡改。如果只有具有相互通信资格的人才拥有密钥,一旦通过报文完整性检测,意味着发送者就是具有报文发送资格的人,也完成了报文发送者的有效身份认证。注意,这种报文发送者有效身份认证只是用于确定发送者是否是具有一定授权的人,和报文数字签名是不同的。

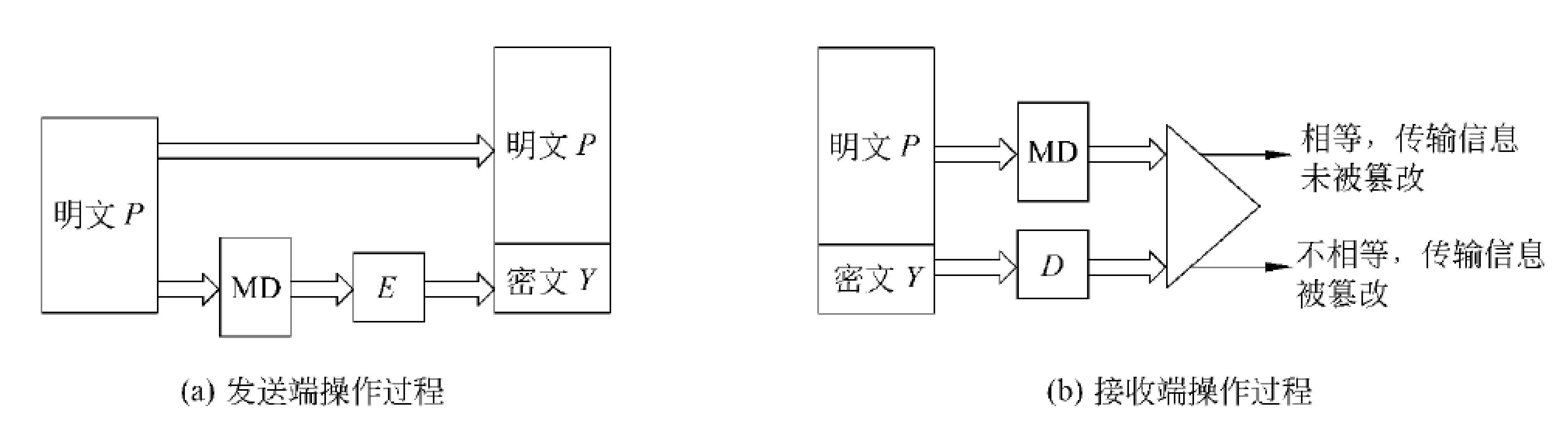


图 3.20　完整性检测和用户身份认证

完成报文摘要和加密、解密运算会增加发送端和接收端的处理负担,简单的报文完整性检测和发送者身份认证过程将报文和密钥串接后再进行报文摘要运算,即 $h=\mathrm{MD}(P \| K)$($\|$ 是将两组信息串接在一起的串接操作符),由于密钥是保密的,即使获得了明文 P,也无法计算出摘要 h。因此,如果接收端对接收到的报文进行同样的运算过程,且运算结果和附在报文后的摘要相同,同样可以证明报文的完整性和发送者的有效身份。散列消息认证码(Hashed Message Authentication Codes,HMAC)就是一种将密钥和报文一起作为数据组的报文摘要算法,运算过程如图3.21所示。

在图3.21中,b 位是数据组的长度,无论是MD5,还是SHA-1,数据组的长度都是512位。n 位是报文摘要的长度,当然也是初始向量的长度,MD5是128位,而SHA-1是160位。如果密钥 K 的长度大于 b 位,则先通过报文摘要运算将其变为 n 位。一般要求密钥 K 的长度大于 n 位,因此,当密钥 K 的长度在 $n \sim b$ 位之间时,通过添加全0的填充位将其扩展到 b 位,图3.21中 $K+$ 就是扩展到 b 位的密钥。ipad由字节36H重复 $b/8$ 次构成,opad由字节5CH重复 $b/8$ 次构成,它们

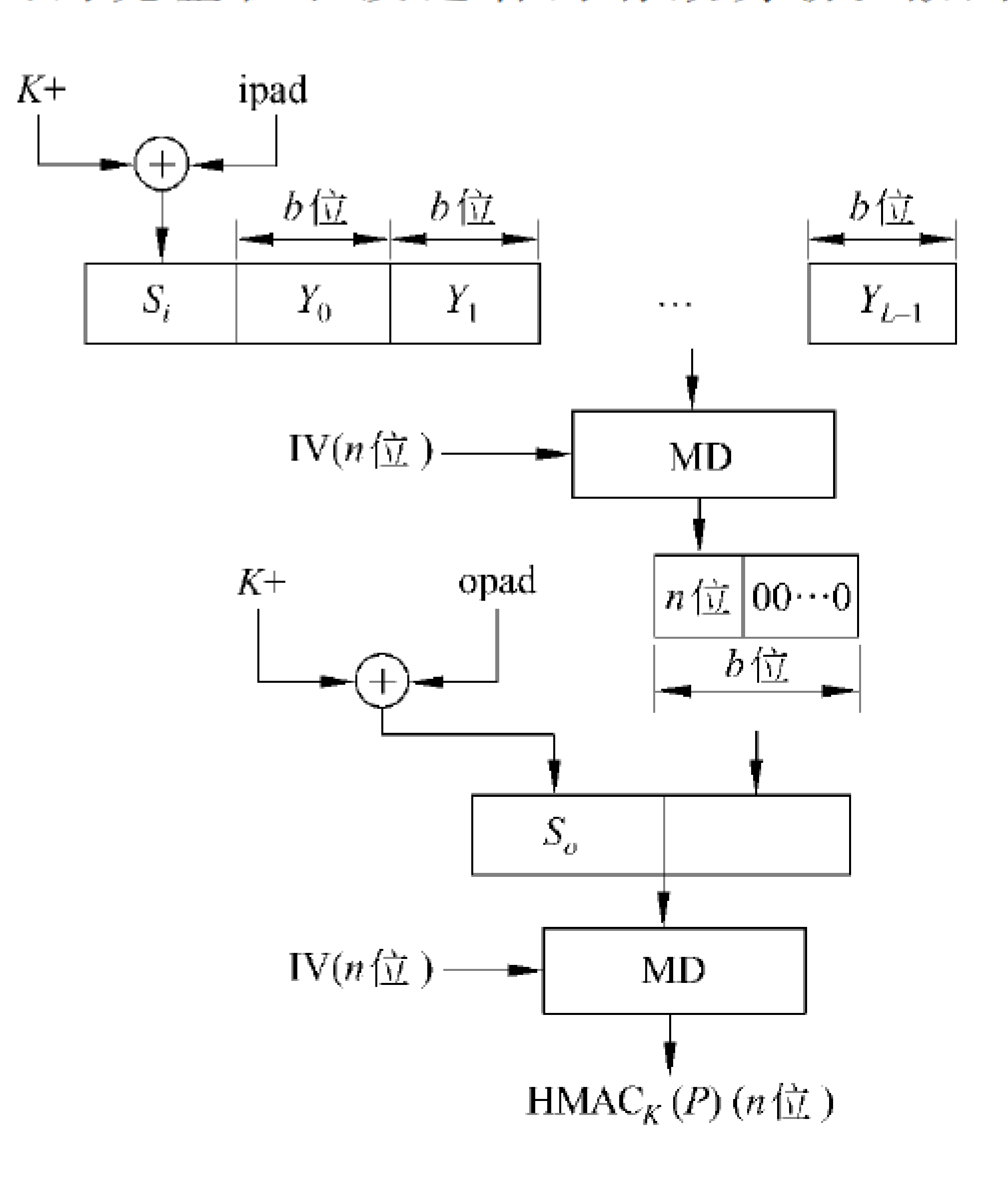


图 3.21　HMAC运算过程

和 K+异或运算后分别构成数据组 S_i 和 S_o。图 3.21 中的报文摘要算法 MD 没有限制，可以是 MD5，或 SHA-1，也可以是其他报文摘要算法，如果采用 MD5 报文摘要算法，表示为 HMAC-MD5-128，采用 SHA-1 报文摘要算法，表示为 HMAC-SHA-1-160，后面的 128 和 160 为基于密钥生成的报文摘要长度。参加第一级报文摘要运算的数据序列由数据组 S_i 串接报文后构成，即 MD((K+⊕ipad) ‖ P)。第一级报文摘要运算的结果(n 位)通过添加全 0 的填充位扩展成 b 位，和 S_o 串接后构成第二级报文摘要运算的输入数据序列，因此，HMAC 的最终结果是 MD((K+⊕opad) ‖ MD((K+⊕ipad) ‖ P))。

3.3 数字签名

在现实世界中，通过印章或亲笔签名来证明真实性，但如何在网络世界确定发送方的真实性呢？数字签名技术就用于解决网络中传输信息的真实性问题，它具有如下特征：

- 接收者能够核实发送者对报文的数字签名；
- 发送者事后无法否认对报文的数字签名；
- 接收者无法伪造发送者对报文的数字签名。

目前存在两种用于数字签名的技术，它们分别基于对称密钥和公开密钥算法。

3.3.1 基于对称密钥算法的数字签名技术

基于对称密钥的数字签名技术如图 3.22 所示。这种技术需要有一个安全、有公信力的权威机构，这个权威机构和所有需要认证的用户都有着对称密钥，当然，不同用户的对称密钥必须是不同的，而且，对称密钥只限于权威机构和用户知道。当用户 A 向用户 B 发送报文，为了证明该报文确实由用户 A 发送，用户 A 先向权威机构发送一组信息，这一组信息包括用明文方式给出的发送者信息用户 A，用用户 A 和权威机构约定的对称密钥 K_A 加密的接收者信息用户 B、报文 P、随机数 R_A 和时间戳 T。当权威机构接收到用户 A 发送给它的这一组信息，用和用户 A 约定的对称密钥 K_A 解密密文，获得用户 A 发送给用户 B 的报文、随机数 R_A 和时间戳 T，权威机构先用只有它知道的密钥 KBB 加密根据用户 A 发送给用户 B 的报文 P 计算出的报文摘要 MD(P)、发送者信息、用户 A 及时间戳 T，然后将密文和发送者信息用户 A、报文 P、随机数 R_A 和时间戳 T 用权威机构和用户 B 约定的对称密钥 K_B 进行加密产生密文，并将密文发送给用户 B。用户 B 用对称密钥 K_B 解密后，得到发送者信息用户 A、报文 P、随机数 R_A 和时间戳 T，及用密钥 KBB 加密后的密文。由于密钥 KBB 只有权威机构知道，用户 B 只能完整保留该密文而无法进行处理。一旦双方就报文的真实性发生争执，如用户 A 否认发送过该报文，或者虽然承认发送过报文，但否认是用户 B 提供的报文内容，用户 B 可将权威机构发送给它的、用密

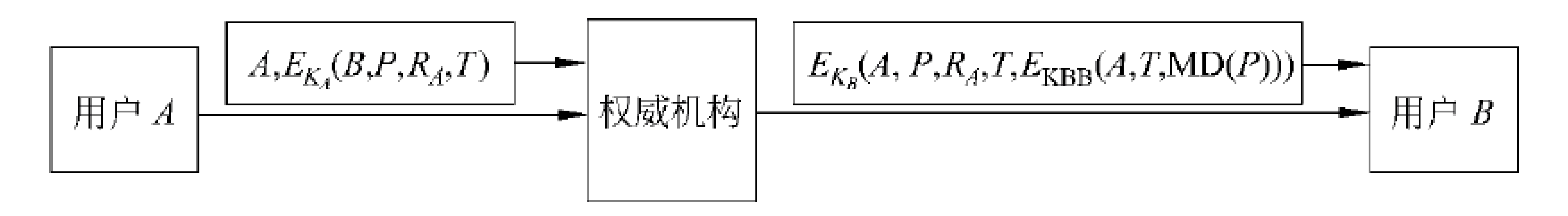


图 3.22 基于对称密钥的数字签名技术

钥 KBB 加密后的密文提交给仲裁机构，仲裁机构要求权威机构对报文 P 的真实性作出判断，权威机构用密钥 KBB 对密文解密，得到发送者信息用户 A、时间戳 T 和报文摘要 MD(P)，对用户 B 提供的报文进行报文摘要运算，并将其结果和解密后得到的报文摘要进行比较，如果相同，且时间戳 T 也相符，仲裁机构将判用户 A 败诉。

用户 A 发送给用户 B 信息中包含时间戳 T 和随机数 R_A 的目的是为了防止中继攻击(亦称重放攻击)，假定用户 C 中间能够截获用户 A 发送给权威机构或权威机构发送给用户 B 的信息，虽然它无法窃取内容，但可以复制下或截留下该信息，经过一段时间后，再一次转发，接收者可用随机数 R_A 来判定是否是已经接收过的报文，用时间戳 T 来判断是否是已经失效的报文，以此防止中继攻击。

基于对称密钥的数字签名技术，先将所有需要数字签名的报文发送给权威机构，再由权威机构转发给接收者，这势必要求权威机构的计算和转发能力极强，而且，一旦权威机构发生问题，整个系统将崩溃。

3.3.2　基于公开密钥算法的数字签名技术

1. 认证中心和 PKI

基于 RSA 公开密钥算法的数字签名技术的实现原理是私钥的秘密性，私钥和公钥的关联性，及公钥的公开性，只要证明某个公钥和用户之间的绑定关系，就可证明和该公钥关联的私钥的拥有者就是该用户，因此，实现基于公开密钥算法的数字签名技术的第一步就是证明公钥和用户之间的绑定关系。用户不能简单地通过公告自己的公钥来宣示自己和公钥的绑定关系，因为这样做既没有公信力，也很容易让某个攻击者伪造和别人的公钥之间的绑定关系。假定用户 B 通过网页来公告自己的公钥 PKB，用户 A 就有可能通过入侵用户 B 的网页，篡改用户 B 在网页中给出的公钥 PKB，将自己的公钥 PKA 作为用户 B 的公钥予以公告。

如何让人们确信某个用户通过网页或媒体公告的公钥不是其他人伪造的？公开密钥算法为解决这种公钥认证问题，设计了认证中心(Certification Authority，CA)。认证中心是一个具有公信力的权威机构，当用户 B 希望通过认证中心来认证它所发布的公钥 PKB 不是伪造时，用户 B 需要携带希望认证的公钥 PKB 和证明自己身份的证件到认证中心，认证中心确认用户 B 的真实身份后，提供一份证书，证书分两部分：一部分是用明文方式给出的用于确认公钥 PKB 和用户 B 之间绑定关系的证明；另一部分是用认证中心的私钥 SKCA 对上述明文的报文摘要进行解密运算后生成的密文(D_{SKCA}(MD(P))。证书含有的主要内容如图 3.23 所示。



图 3.23　证书格式

- 版本：证书格式的版本号，目前最新版本是版本 3。
- 证书序号：认证中心用于唯一标识该证书的序号。
- 签名算法标识符：用于标识证书签名算法及算法相关的参数。

- 签发者名称：签发该证书的认证中心名称。
- 起始时间：证书有效的起始时间。
- 终止时间：证书有效的终止时间。
- 用户名称：证明和证书中给出的公钥有绑定关系的用户名称。
- 用户公钥信息：和证书指定用户有绑定关系的公钥及公钥所相关的算法和参数。
- 签发者唯一标识符：在签发者名称可能重名的情况下用于唯一标识签发该证书的认证中心。
- 用户唯一标识符：在用户名称可能重名的情况下用于唯一标识和证书中给出的公钥有绑定关系的用户。
- 扩展信息：用于给出其他一些相关信息。
- 认证中心签名：用认证中心的私钥对证书内容的报文摘要进行解密运算：$D_{SKCA}(MD(P))$，P 是证书内容。

认证中心的作用是证明公钥和用户的绑定关系，因此，认证中心本身就是证书检索中心，用户可以通过检索证书库来获得任何一个注册用户的证书。同时，认证中心也对证书进行管理，如注销已经失效的证书，或是撤销用户因为担心私钥泄密而要求停止使用的证书。多数情况下，认证中心还负责为用户生成私钥和公钥对，并根据为用户生成的公钥自动生成证书，一方面将证书提供给用户，另一方面直接将证书归档，以便其他用户检索。同时通过适当方式向用户提供私钥。由于私钥代表着用户本身，类似银行账号和口令，认证中心必须有一套可靠的机制来保证私钥的安全，如银行为用户提供 USBkey 的机制。认证中心是用户向外发布证书的主要渠道，当然，用户也可通过其他渠道，如网页或媒体发布证书。这种证书是无法伪造的，假定用户 A 进入用户 B 的主页，想用自己的公钥 PKA 取代证书上的公钥 PKB，用户 A 只能篡改明文，无法修改密文。当用户 C 访问到已被用户 A 篡改的证书后，用户 C 将用认证中心的公钥 PKCA 对证书的密文进行加密运算($E_{PKCA}(D_{SKCA}(MD(P)))=MD(P)$)，如果发现用认证中心的公钥 PKCA 对证书的密文进行加密运算后得到的明文的报文摘要和通过对证书中给出的明文进行的报文摘要运算后得到的结果不一致，就认为该证书已被篡改。认证中心的公钥 PKCA 可以通过多种有公信力的渠道公告给广大用户，因此，认证中心的公钥 PKCA 是无法伪造的。当然，全国乃至全球不可能只有一个认证中心，应该有多个负责一个地区，或一个城市的认证中心。但某个城市的用户如何确认另一个城市的认证中心提供的证书？在上面的讨论中，通过众所周知的认证中心的公钥 PKCA 来验证证书的真伪，那么，所有认证中心能否使用相同的公钥 PKCA 和私钥 SKCA 对？结论当然是否定的，这将对安全带来很大的隐患。但不同认证中心使用不同的公钥和私钥对带来的问题是如何保证用户获得的某个认证中心的公钥不是伪造的。公开密钥设施(Public Key Infrastructure，PKI)采用如图 3.24 所示的分层认证结构，分层认证结构由一个根认证中心和若干层认证中心组成，每一层认证中心提供的公钥由上一层认证中心予以认证，根认证中心提供的公钥通过有公信力的多种渠道予以公告。在实际操作过程中，每一层认证中心提供的公钥都可通过这一层所管辖地区的、有公信力的传播媒体予以公告，如负责江苏地区的认证中心，可以通过江苏省电视台、政府报纸公告其公钥，而负责南京地区的认证中心可以通过南京市电视台、南

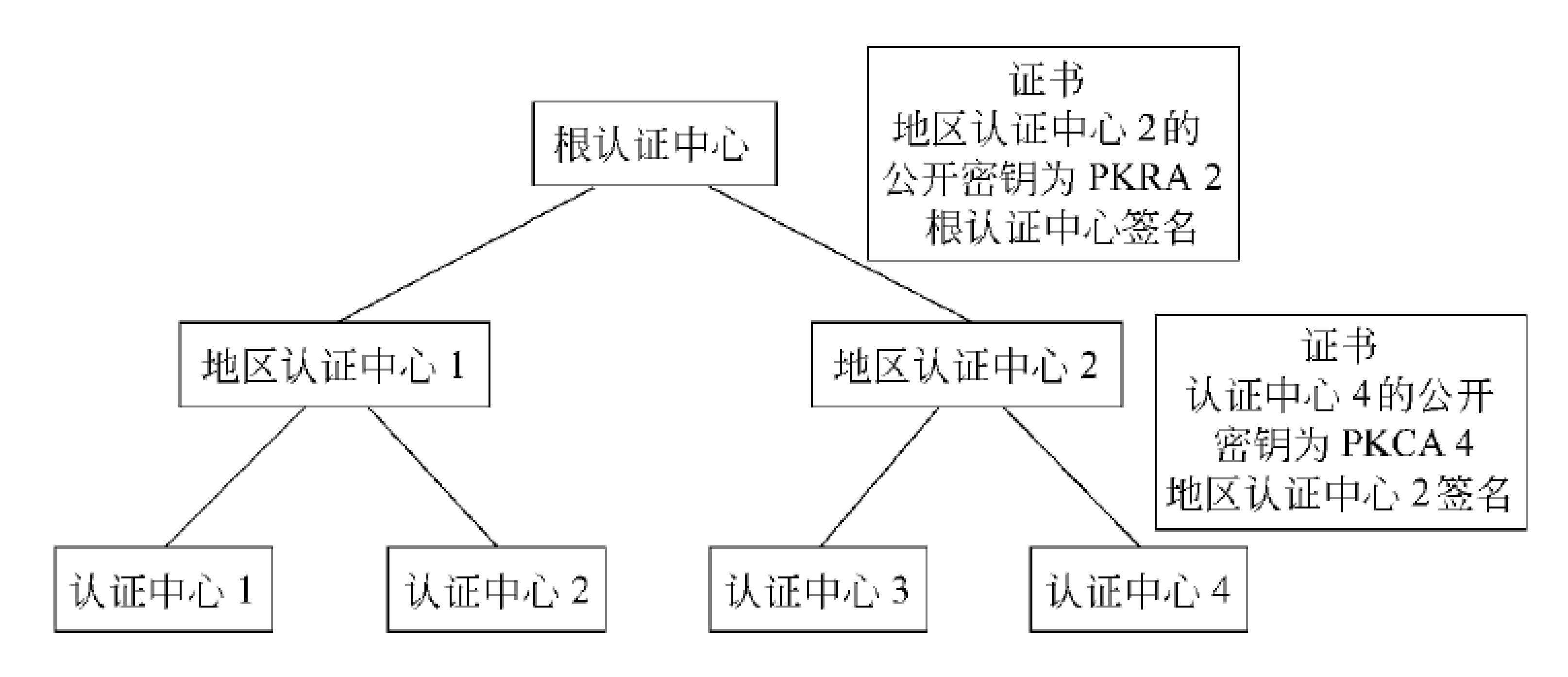


图 3.24　分层认证结构

京市政府报纸予以公告。但当某个苏州地区的用户 A 希望和南京地区的用户 B 通信时，发现用户 B 的公钥有南京市认证中心颁发的证书，为验明证书的真伪，它需要获得南京市认证中心的公钥。为了可靠，它可以要求南京市认证中心提供证明其和该公钥之间绑定关系的证书，该证书应由上一层认证中心(江苏省认证中心)签发。由于用户 A 通过有公信力的媒体，已经获得江苏省认证中心的公钥，就可以用江苏省认证中心的公钥来证明南京市认证中心提供的证明其和该公钥之间绑定关系的证书的真伪。在确认了南京市认证中心的公钥后，就可证明用户 B 的公钥的真伪了。用 Y＜＜X＞＞表示由认证中心 Y 签发用于证明用户 X 和某个公钥之间绑定关系的证书，那么，苏州市用户 A 和南京市用户 B 相互确认对方公钥的过程如下。

用户 A 确认用户 B 公钥过程：

江苏省认证中心＜＜南京市认证中心＞＞ 南京市认证中心＜＜用户 B＞＞

用户 B 确认用户 A 公钥过程：

江苏省认证中心＜＜苏州市认证中心＞＞ 苏州市认证中心＜＜用户 A＞＞

这样的认证过程构成认证链。

2. 数字签名过程

公开密钥算法中的私钥具有私密性，只有用户本身才知道，而公钥和用户之间的绑定关系又经过认证中心的认证，具有不可否认性。因此，当用户 A 向用户 B 发送明文 P，它可以用自己的私钥对明文 P 进行解密运算，如果接收端用用户 A 公告的公钥进行加密运算后，能够还原成明文 P，则可断定，该明文由用户 A 发送，且明文为 P，整个数字签名认定过程如图 3.25 所示。

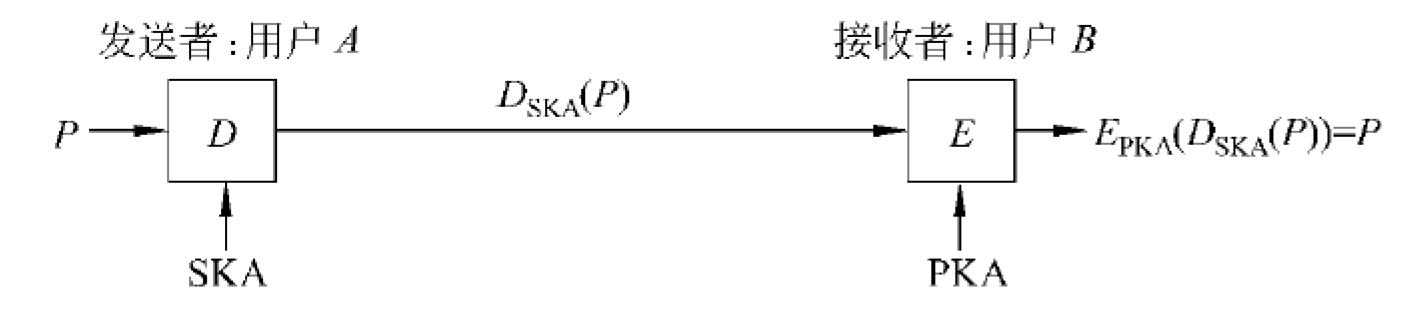


图 3.25　基于公开密钥算法的数字签名技术

常规的基于公开密钥算法的加密、解密过程，是发送者用公钥加密，接收者用私钥解密，$D_{SKA}(E_{PKA}(P))=P$，这样，由于私钥是不公开的，只有拥有私钥的用户才能对密文解

密，因此，密文对其他用户是保密的。虽然公开密钥算法中的公钥和私钥是不同的，且不能由公钥推算出私钥，但加密、解密算法可以对调，即 $E_{PKA}(D_{SKA}(P))=D_{SKA}(E_{PKA}(P))=P$，因此，图 3.25 用私钥对明文进行解密运算后得到的密文 $D_{SKA}(P)$，用公钥对其进行加密运算后，仍然还原成明文 $P(E_{PKA}(D_{SKA}(P))=P)$。由于公钥没有私密性，所有知道发送者公钥的人均可获得明文 P，因此，图 3.25 解决了报文鉴别问题，但没有解决报文的保密性问题。

既解决报文鉴别，又解决报文保密性问题的发送、接收过程如图 3.26 所示，明文在发送时，先用发送者(用户 A)的私钥进行解密运算，然后再用接收者(用户 B)的公钥对解密运算后得到的密文进行加密运算。接收者进行相反操作，先用接收者(用户 B)的私钥对密文进行解密运算，得到用发送者(用户 A)私钥进行解密运算后得到的密文，如果能用用户 A 的公钥对其进行加密运算后，还原出明文 P，则证明该明文是由用户 A 发送的。

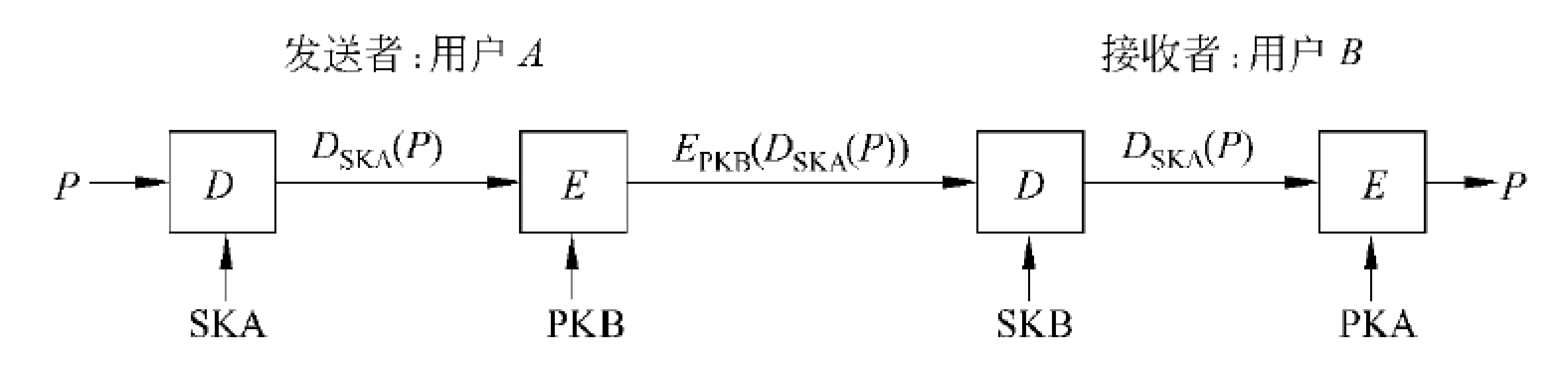


图 3.26 基于公开密钥算法的数字签名技术

对于图 3.26 所示的操作过程，由于只有用户 B 才能还原出 $D_{SKA}(P)$，因此，尽管 PKA 和加密算法是公开的，也只有用户 B 最终能获取明文 P，解决了报文的保密性问题。

根据目前的计算能力，某个用户用数字签名技术对另一个用户进行栽赃的可能性是不存在的，任何用户无法事先伪造一个密文 Y，然后用另一个用户的公钥 PK 对伪造的密文 Y 进行加密运算，得到预期的、不利于另一个用户的明文 P。但任何信息用某个用户的公钥 PK 进行加密运算后都有结果，虽然这种结果毫无意义，但从原理讲，这种结果都可认定是该用户发送的明文。为了防止这种无聊的操作产生不良的后果，应该对数字签名的认定过程加一些限制。如图 3.27 所示，用户 A 用私钥 SKA 对明文 P 经过报文摘要运算后得到的摘要 MD(P)进行解密运算，产生数字签名(D_{SKA}(MD(P))，将明文 P 和数字签名一同发送给用户 B。用户 B 认定明文 P 是用户 A 发送的前提是：用用户 A 对应的公钥 PKA 对数字签名进行加密运算后得到的结果和对明文 P 进行报文摘要运算后得

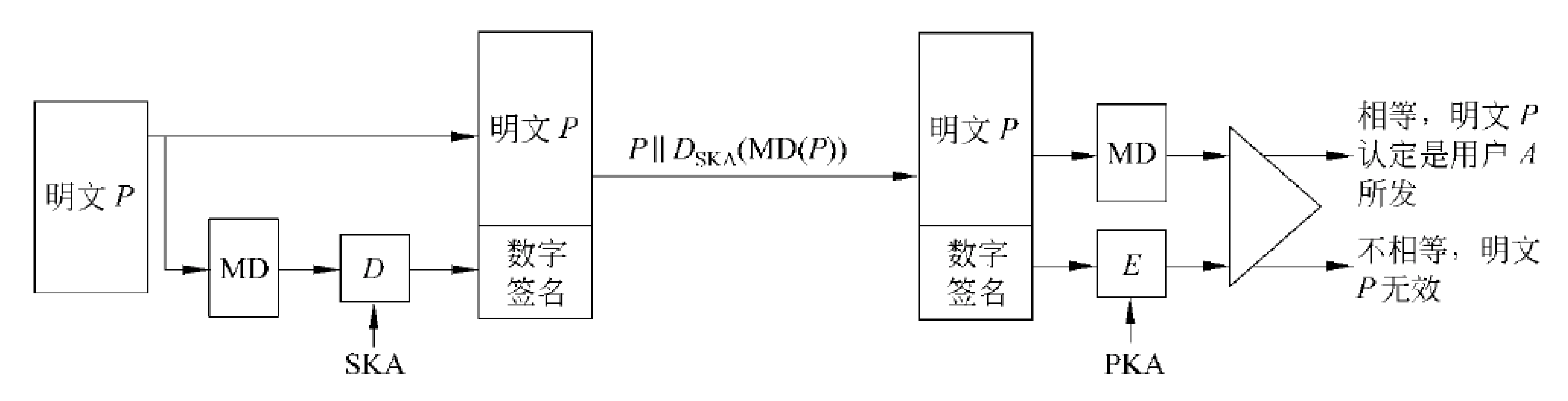


图 3.27 改进后的数字签名认定过程

到的结果相同，即 E_{PKA}(数字签名)＝MD(P)。图3.27所示的数字签名认定过程，既避免对整个明文 P 进行加密运算，又通过数字签名和明文 P、发送者私钥SKA之间的关联将明文 P 和发送者绑定在一起。当然，如果既要实现数字签名，又要实现报文传输的保密性，发送端仍然需要用用户 B 的公钥对明文 P 和数字签名进行加密运算，用户 B 接收到密文后，首先通过私钥和解密运算还原出明文 P 和数字签名。

3.4 认证协议

认证过程就是确认通信另一方的身份的过程，因此，认证协议就是一种保证接收者只接收授权者发送的数据的机制，数字签名技术由于在数据中携带了可以唯一标识发送者、且别人无法伪造的标识信息(数字签名)，使得接收者能够根据标识信息确认发送者身份，并因此确定是否是授权者发送的数据，可以作为认证机制，但数字签名技术中强调的接收者无法伪造标识信息的特点在认证过程中属于多余的要求，而且这种多余的要求会增加认证机制的复杂性，因此，单纯的认证机制一般不采用数字签名技术。

3.4.1 Kerberos

基于对称密钥加密算法的认证机制比较简单，假定服务器 S 提供有偿服务，因此，所有希望得到服务器 S 服务的客户都需要事先注册到服务器 S，并分配一个客户和服务器 S 共享的对称密钥 $K_{C,S}$，当然，不同客户分配的对称密钥都是不同的，服务器 S 建立一个注册信息库，库中对每一个注册客户都记录下客户名和对应的对称密钥，为了安全，对称密钥不以明文方式存放。当客户 C 请求服务器 S 的服务时，客户 C 发送的请求消息中包含认证信息，如图3.28所示，认证信息是对客户名 ID_C、客户IP地址 AD_C 和序号SEQ用客户和服务器 S 共享密钥 $K_{C,S}$ 加密运算后的密文($E_{K_{C,S}}(ID_C \| AD_C \| SEQ)$)。服务器 S 接收到客户 C 发送的服务请求后，用服务请求中给出的客户名 ID_C 检索注册信息库，找到该客户对应的共享密钥 $K_{C,S}$，用共享密钥 $K_{C,S}$ 解密认证信息，如果认证信息包含的客户名、客户IP地址和服务请求中给出的客户名、源IP地址相同，表示服务请求是授权用户客户 C 发送的，否则，拒绝该服务请求。序号用于防止中继攻击。

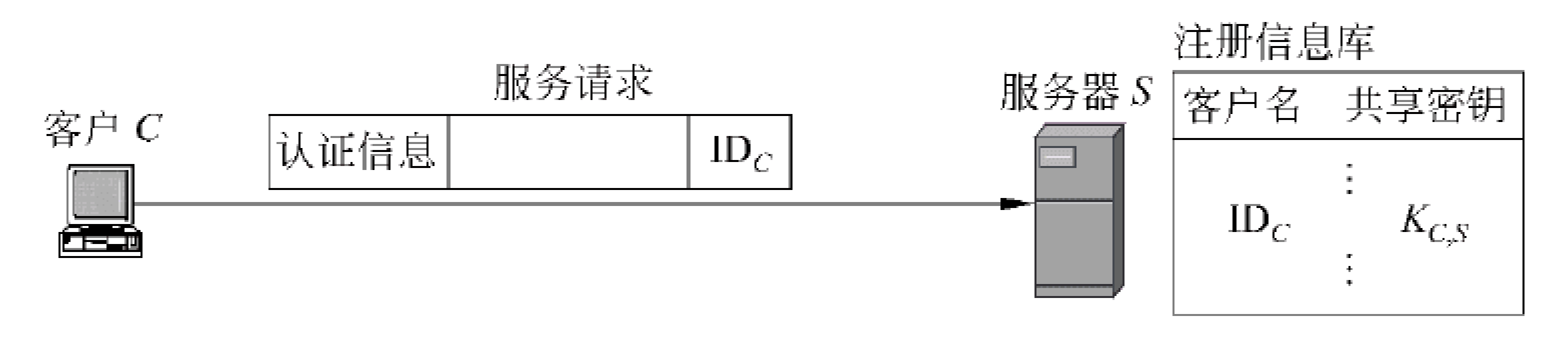


图3.28 基于对称密钥加密算法的认证机制

图3.28所示的基于对称密钥加密算法的认证机制由应用服务器实现认证客户的功能，每一个应用服务器都需建立包含所有授权用户信息的注册信息库，实际应用中，某个客户可能是多个应用服务器的授权客户，因此，需要向多个应用服务器进行注册，多个应用服务器都需包含该客户的有关信息，这不仅给用户带来麻烦，而且也加重应用服务器的负担。根据分工合作的原则，应该由独立的认证服务器来完成对客户的认证功能，应用服

务器不再存储授权用户的信息，这种基于对称密钥加密算法，且又采用独立认证服务器的认证机制就是 Kerberos。

1. 身份认证

图 3.29 所示的 Kerberos 认证过程中除了应用服务器 V 外，还采用了两个认证用的服务器，一个认证服务器 AS，用于确认客户身份，另一个是通行证签发服务器 TGS，用于确认客户是否授权访问某个应用服务器。当客户 C 希望访问应用服务器 V 时，它首先需要认证服务器 AS 完成对其身份的认证，客户 C 发送给认证服务器 AS 的认证请求中包含客户名 ID_C、通行证签发服务器名 ID_{TGS} 和这一次认证的有效时间 TIMES(通常以起始和终止时间方式给出有效时间)，在有效时间内，客户 C 可以一直使用本次认证结果。认证服务器 AS 通过检索注册信息库 1 找到客户名 ID_C 及对应口令 PW_C，只要确认客户 C 知道口令 PW_C，就可断定客户 C 的客户名为 ID_C。认证服务器通过口令 PW_C 推出密钥 K_C，同时，产生一个认证密钥 $K_{C,TGS}$，一方面用 K_C 加密认证密钥 $K_{C,TGS}$，另一方面将 $K_{C,TGS}$ 包含在用认证服务器 AS 和通行证签发服务器 TGS 的共享密钥 K_{TGS} 加密的通行证 $Ticket_{TGS}$ 中，由于 $Ticket_{TGS}$ 只能由通行证签发服务器 TGS 解密，而只有知道口令 PW_C 的客户才能解密用 K_C 加密的密文，因此，拥有 $Ticket_{TGS}$ 包含的 $K_{C,TGS}$ 的客户即是客户名为 ID_C 的客户。因此，客户身份认证过程中，认证服务器 AS 返回给客户 C 的认证响应中主要包含两部分信息：$E_{K_C}(K_{C,TGS} \| TIMES \| Nonce1 \| ID_{TGS})$ 和 $E_{K_{TGS}}(K_{C,TGS} \| ID_C \| AD_C \| TIMES)$，第一部分信息保证只有知道口令 PW_C 的客户才能获得认证密钥 $K_{C,TGS}$，第二部分信息将客户名 ID_C、客户 IP 地址 AD_C、身份有效时间 TIMES 和认证密钥 $K_{C,TGS}$ 绑定在一起。随机数 Nonce1 用于匹配客户发送的认证请求和认证服务器发送的认证响应。

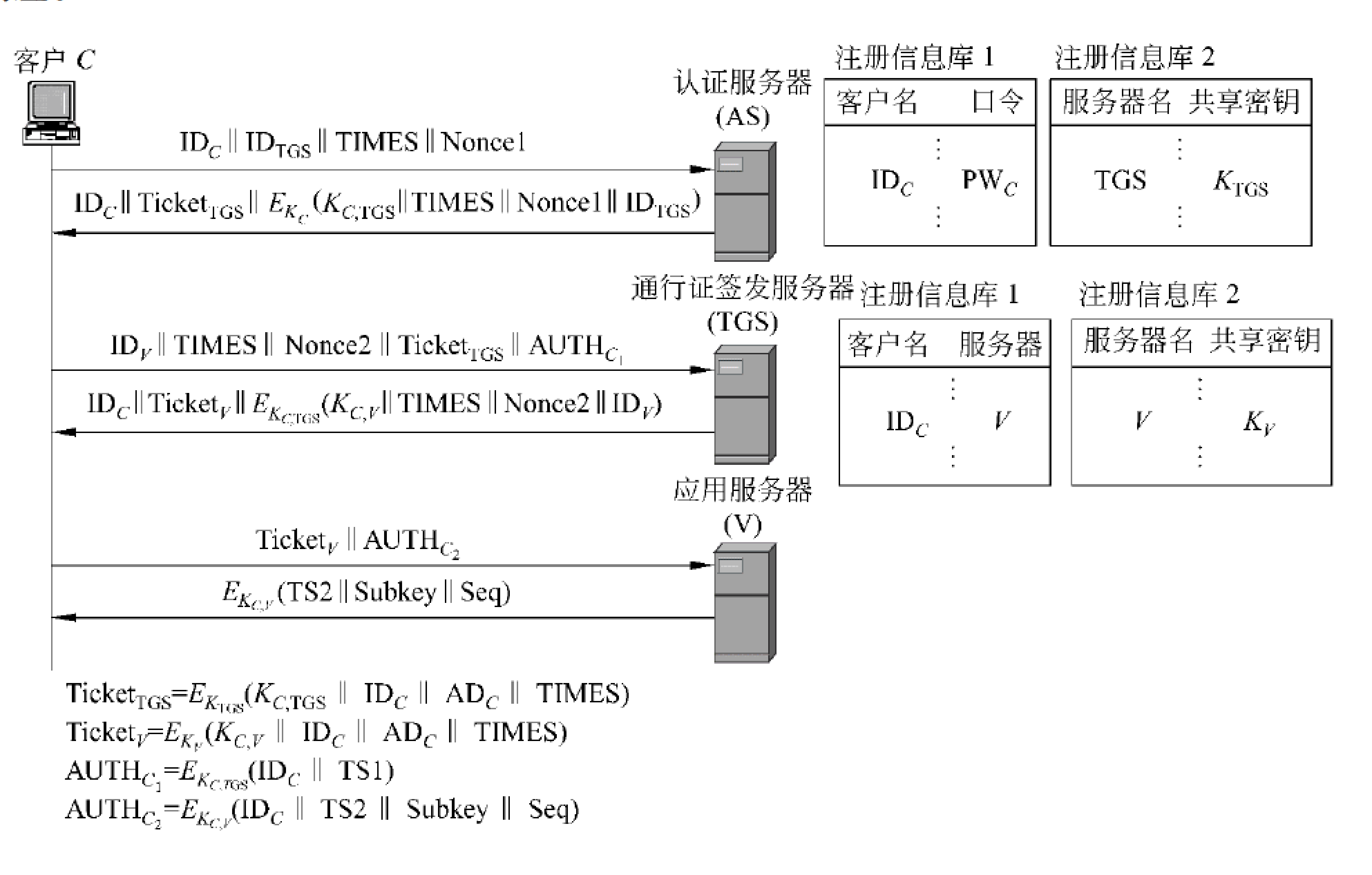


图 3.29 Kerberos 认证过程

2. 获取服务通行证

认证服务器只负责客户身份认证，判断客户是否有获得指定服务的授权的功能由通行证签发服务器 TGS 完成，客户向通行证签发服务器发送的服务通行证请求中包含提供指定服务的服务器名 ID_V，认证服务器提供的签发服务器通行证 $Ticket_{TGS}$ 和认证信息 $AUTH_{C1}$，认证信息是用认证密钥 $K_{C,TGS}$ 加密客户名 ID_C 和用于防止中继攻击的时间 TS1 后得到的密文。通行证签发服务器用密钥 K_{TGS} 解密 $Ticket_{TGS}$，获得认证密钥 $K_{C,TGS}$，然后用 $K_{C,TGS}$ 解密客户发送的认证信息 $AUTH_{C1}$，如果解密后得到的明文中包含的客户名和 $Ticket_{TGS}$ 中包含的客户名相同，客户身份通过认证。在完成客户身份认证后，通过检索注册信息库 1 判定客户是否授权访问 ID_V，同时通过检索注册信息库 2 获得通行证签发服务器 TGS 和服务器 ID_V 的共享密钥 K_V。为了让服务器 ID_V 能够认证客户身份，产生用于服务器认证客户的认证密钥 $K_{C,V}$，一方面将认证密钥包含在用 K_V 加密后产生的表示客户授权访问服务器 ID_V 的通行证 $Ticket_V$ 中，另一方面用签发服务器认证客户的认证密钥 $K_{C,TGS}$ 加密 $K_{C,V}$，这样就保证了只有服务器 ID_V 和客户名为 ID_C 的客户才有可能拥有认证密钥 $K_{C,V}$，只要服务器 ID_V 确认某个客户拥有认证密钥 $K_{C,V}$，可断定该客户是客户名为 ID_C 的客户。因此，获取服务通行证过程中，通行证签发服务器返回给客户 C 的服务通行证响应中主要包含两部分信息：$E_{K_{C,TGS}}(K_{C,V} \| \text{TIMES} \| \text{Nonce2} \| ID_V)$ 和 $E_{KV}(K_{C,V} \| ID_C \| AD_C \| \text{TIMES})$，第一部分信息保证只有拥有认证密钥 $K_{C,TGS}$ 的客户才能获得服务器 ID_V 认证客户的认证密钥 $K_{C,V}$，第二部分信息将客户名 ID_C、客户 IP 地址 AD_C、身份有效时间 TIMES 和认证密钥 $K_{C,V}$ 绑定在一起。随机数 Nonce2 用于匹配客户发送的认证请求和认证服务器发送的认证响应。

3. 访问服务器

客户 C 允许访问服务器 ID_V 的前提是获得签发通行证服务器签发的允许访问服务器 ID_V 的通行证 $Ticket_V$，同时须证明自己的客户名为 ID_C，因此，客户 C 向服务器 ID_V 发送的服务请求中，除了签发通行证服务器签发的允许访问服务器 ID_V 的通行证 $Ticket_V$ 外，还有作为认证信息的用认证密钥 $K_{C,V}$ 加密客户名 ID_C 和时间 TS2 后产生的密文。服务器 ID_V 用密钥 K_V 解密允许访问服务器 ID_V 的通行证 $Ticket_V$，得到客户名 ID_C、客户 IP 地址 AD_C 和认证密钥 $K_{C,V}$。然后，用认证密钥 $K_{C,V}$ 解密客户的认证信息，如果解密后得到的客户名 ID_C 和通行证中的客户名相同，表明该客户确实是客户名为 ID_C 的客户，对其请求的服务予以响应。如果客户 C 希望对和服务器 ID_V 之间传输的服务请求和响应进行加密，可以在认证信息中给出会话密钥。如果客户 C 希望对服务器 ID_V 的身份予以认证，则由服务器 ID_V 在服务响应中给出作为认证信息的用认证密钥 $K_{C,V}$ 加密 TS2 后得到的密文。TS2 的作用同样是为了防止中继攻击。

3.4.2 TLS

为了对客户和服务器之间传输的数据进行加密和认证，客户和服务器之间必须约定加密密钥和认证密钥、加密算法和认证算法，当然，客户可以通过注册过程和服务器约定上述参数，如果这样，服务器必须为每一个注册客户保留上述安全参数，这一方面增加了服务器的存储负担，另一方面也增加了泄密这些安全参数的可能性，因此，有必要为每一

次客户和服务器之间的数据传输过程动态产生上述安全参数，而且这些安全参数在每一次数据传输过程结束后自动失效，这将大大增强了客户和服务器之间数据传输的安全性，但必须有一套用于对双方身份进行认证并协商安全参数的协议，运输层安全(Transport Layer Security，TLS)就是这样一种协议。

1. TLS 协议结构

TLS 协议结构如图 3.30 所示，TLS 记录协议用于封装上层协议消息，通过 TLS 记录协议传输的上层消息可以实现保密性和完整性，TLS 记录协议封装过程如图 3.31 所示，封装后的记录格式如图 3.32 所示。



图 3.30 TLS 协议结构

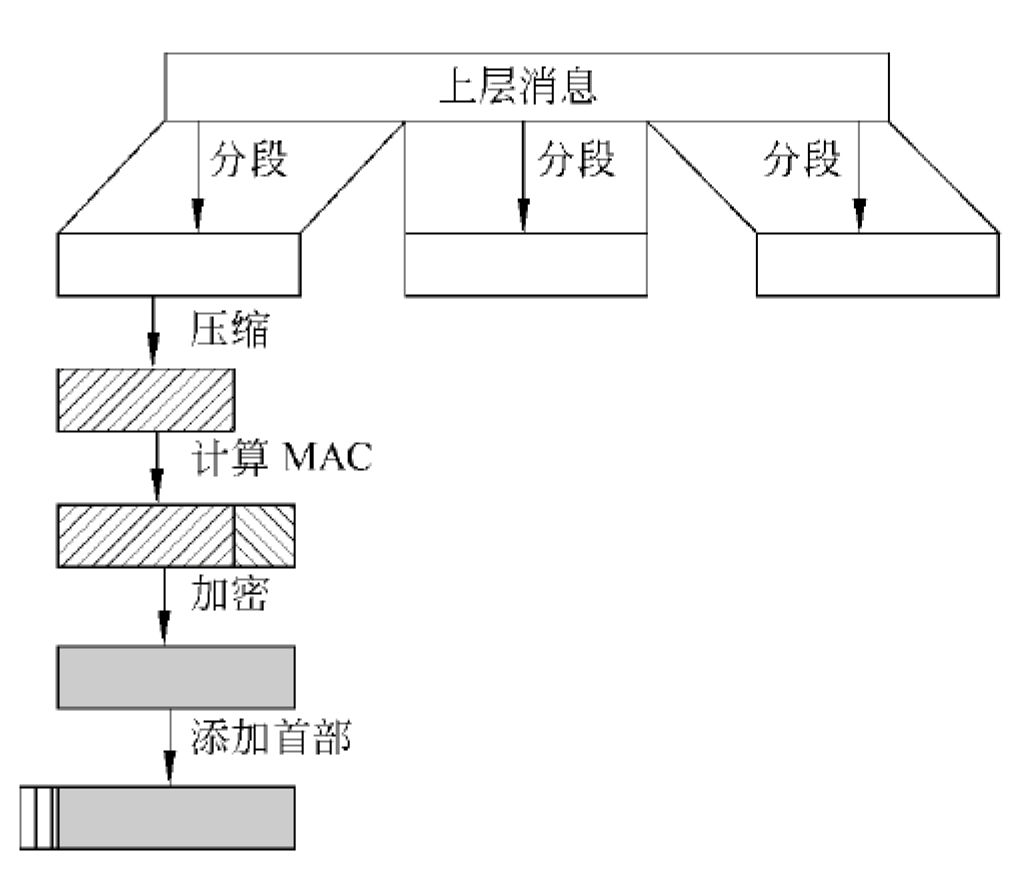


图 3.31 TLS 记录协议封装过程

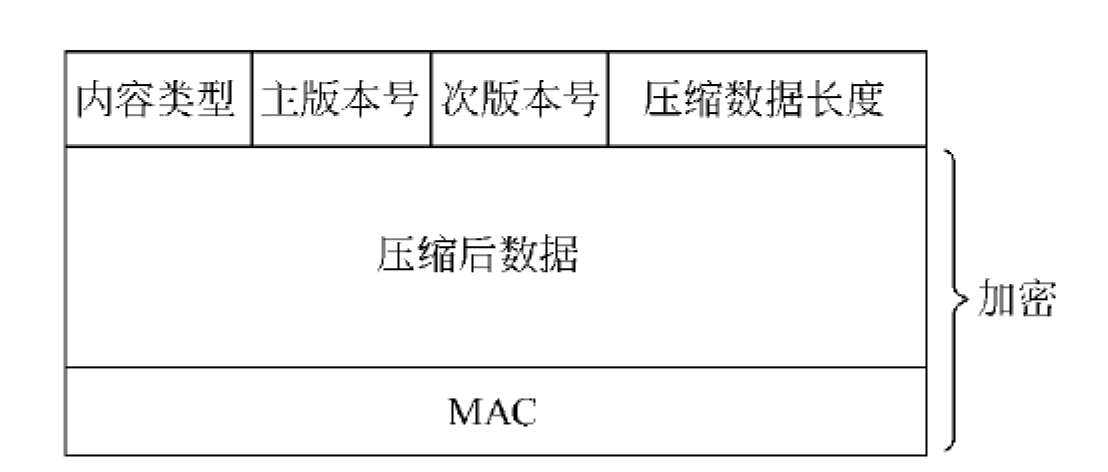


图 3.32 TLS 记录格式

- 内容类型：上层消息类型，如 TLS 握手协议消息、HTTP 消息等。
- 主版本号：对于 TLS，固定为 3。
- 次版本号：对于 TLS，固定为 1。
- 压缩长度：加密操作前上层消息长度。

由于上层消息的长度可以任意，但 TLS 压缩后的数据的长度不能超过 2^{14}B，当单个 TLS 记录协议报文无法容纳上层消息时，必须对上层消息分段，保证每一段上层消息能够封装成单个 TLS 记录协议报文。如果通信双方需要对传输的数据进行加密和完整性检测，必须根据压缩后的数据计算消息认证码(Message Authentication Code，MAC)，并对压缩后的数据和 MAC 进行加密运算，这就要求通信双方在进行图 3.31 所示的封装过程前，完成对方身份认证、压缩算法、加密算法、MAC 算法、加密密钥、MAC 密钥等安全

参数协商，TLS握手协议就是一种实现身份认证和安全参数协商的协议。通信双方约定新的安全参数后，通过安全参数切换协议通知对方开始使用新约定的安全参数。报警协议用于传输出错消息，如解密失败、无法确认证书等。通信双方第一次启动握手协议时，初始安全参数为不压缩、不加密、不计算MAC。

图3.30所示的协议结构中，用TCP协议来传输TLS记录协议报文，这是基于客户和服务器是互联网上相隔多个不同类型的传输网络的两个终端的情况，这种情况下，只有IP分组才能实现端到端传输，而且只有通过TCP才能实现端到端的可靠、按序传输。如果客户和服务器是连接在同一传输网络上的两个端点，如连接在同一以太网上的两个端点，未必需要用TCP作为TLS记录协议报文的承载协议。

2. 握手协议实现认证和安全参数协商过程

握手协议操作过程如图3.33所示，整个操作过程分为四个阶段，阶段1用于双方对压缩算法、加密算法、MAC算法及TLS协议版本达成一致。客户C在客户Hello消息中按优先顺序列出客户C支持的算法列表及TLS协议版本，服务器V从客户C支持的算法列表中按优先顺序选择一种自己支持的算法作为双方约定的算法，在双方支持的TLS版本中选择较低的TLS版本作为双方约定的TLS版本，并通过服务器Hello消息将双方约定的算法、TLS版本回送给客户C。

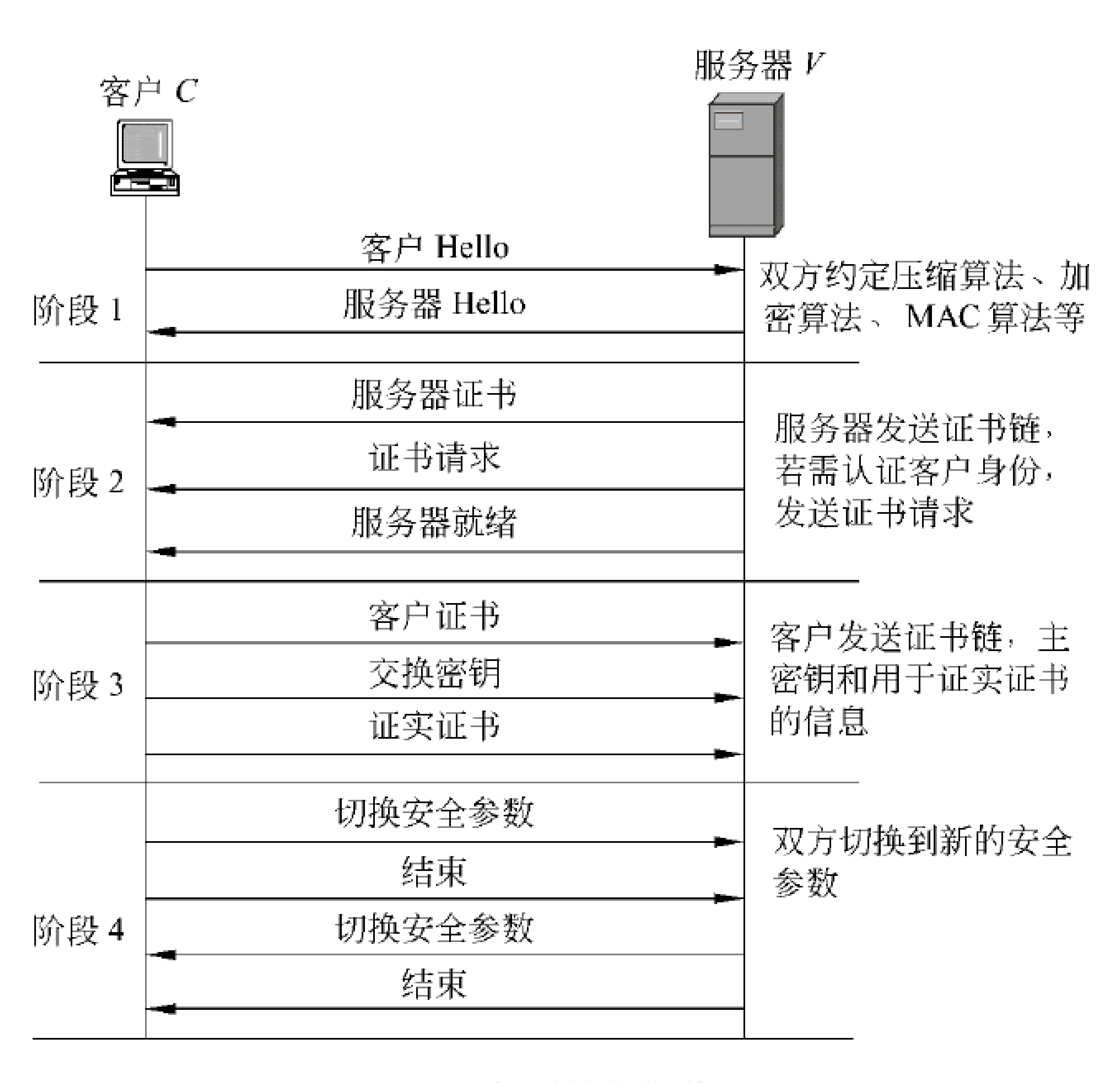


图3.33 握手协议操作过程

阶段2用于完成对服务器V的身份认证。TLS支持多种认证服务器V身份的机制，这里以基于公开密钥算法的认证机制为例讨论服务器V身份的认证过程。服务器V身份认证过程就是确认客户C访问的服务器V就是域名为ID_V的服务器的过程。基于公开密钥算法认证服务器V的过程如下：服务器V向客户C提供由认证中心签发的、证明

ID_V 和公钥 PKV 之间绑定关系的证书，对于图 3.34 所示的认证中心结构，由于客户 C 无法证明认证中心 G 的公钥的合法性，因此，即使接收到认证中心 G 签发的证书，也无法就此断定公钥 PKV 和 ID_V 之间的绑定关系。从图 3.34 可以看出，客户 C 已经证明了认证中心 A 的公钥的合法性，否则无法证明证书链中认证中心 B 的公钥的合法性，并因此无法证明认证中心 D 和 E 的公钥的合法性。因此，服务器 V 通过服务器证书消息提供给客户 C 的是证书链 A＜＜C＞＞、C＜＜G＞＞、G＜＜服务器 V＞＞，客户 C 根据证书链断定公钥 PKV 和 ID_V 之间的绑定关系。断定公钥 PKV 和 ID_V 之间的绑定关系并不能证明服务器 V 和 ID_V 之间的绑定关系，只有在证明了服务器 V 拥有和公钥 PKV 对应的私钥 SKV 后，才能证明服务器 V 的域名为 ID_V。因此，阶段 2 并没有完成对服务器 V 的身份认证。如果服务器 V 需要认证客户 C 的身份，向客户 C 发送证书请求消息，在证书请求消息中，给出服务器 V 拥有的证书链，便于客户 C 发送能够使服务器 V 断定客户 C 身份 ID_C 和公钥 PKC 之间绑定关系的证书链。服务器 V 通过服务器就绪消息结束阶段 2 向客户 C 发送消息的过程。

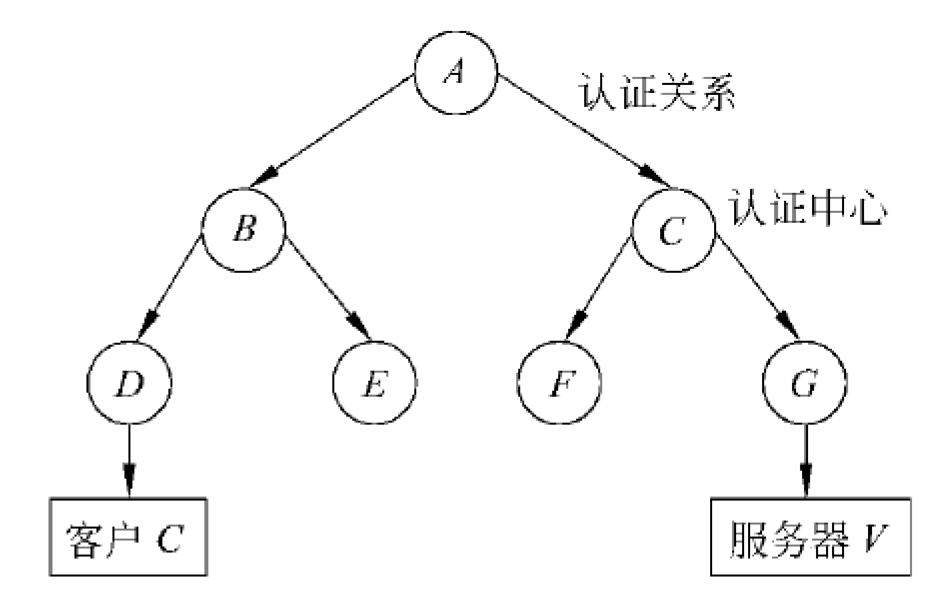


图 3.34 认证中心结构

如果服务器 V 要求认证客户 C 的身份，阶段 3 一开始就由客户 C 通过客户证书消息向服务器 V 发送证书链，证书链包含的证书保证服务器 V 能够断定 ID_C 和公钥 PKC 之间的绑定关系。对于图 3.34 所示的认证中心结构，如果服务器 V 在证书请求消息中给出的证书链是 A＜＜C＞＞、C＜＜G＞＞，则客户 C 向服务器 V 发送的证书链必须是 A＜＜B＞＞、B＜＜D＞＞、D＜＜客户 C＞＞，在双方事先均已证明认证中心 A 的公钥的合法性的前提下，服务器 V 能够根据客户 C 发送的证书链断定 ID_C 和公钥 PKC 之间的绑定关系。客户 C 为了确认服务器 V 拥有和公钥 PKV 对应的私钥 SKV，用公钥 PKV 加密客户 C 选择的预主密钥 PMK($Y=E_{\mathrm{PKV}}(\mathrm{PMK})$)，并通过交换密钥消息将密文 $E_{\mathrm{PKV}}(\mathrm{PMK})$ 发送给服务器 V，由于预主密钥是计算其他密钥的基础，因此，只有双方具有相同的预主密钥才能保证双方产生相同的安全参数，而服务器 V 得到预主密钥的唯一前提是拥有和公钥 PKV 对应的私钥 SKV($D_{\mathrm{SKV}}(Y)=D_{\mathrm{SKV}}(E_{\mathrm{PKV}}(\mathrm{PMK}))=\mathrm{PMK}$)。这就保证只要双方成功协商安全参数，意味着客户 C 访问的就是域名为 ID_V 的服务器。同样，客户 C 发送的证书链只能证明 ID_C 和公钥 PKC 之间的绑定关系，证明客户 C 的用户名为 ID_C，还需证明客户 C 拥有和公钥 PKC 对应的私钥 SKC。为了证明这一点，客户 C 发送的证实证书消息中包含客户 C 用私钥 SKC 对双方交换的握手协议消息的报文摘要进行解密运算后得到的密文($Y=D_{\mathrm{SKC}}(\mathrm{MD}(\text{握手协议消息}))$)。由于服务器 V 保留了双方交换的握手协议消息，通过将密文用 PKC 加密运算后的结果和自己对保留的双方交换的握手协议消息报文摘要运算后的结果进行比较，就可断定客户 C 是否拥有 SKC。比较过程如图 3.35 所示。

客户 C 和服务器 V 首先根据预主密钥 PMK、客户 Hello 和服务器 Hello 消息中包含的客户随机数 Nonce$C$ 和服务器随机数 Nonce$V$ 计算主密钥 MK，在讨论主密钥计算公式前，先讨论几个函数的计算过程。

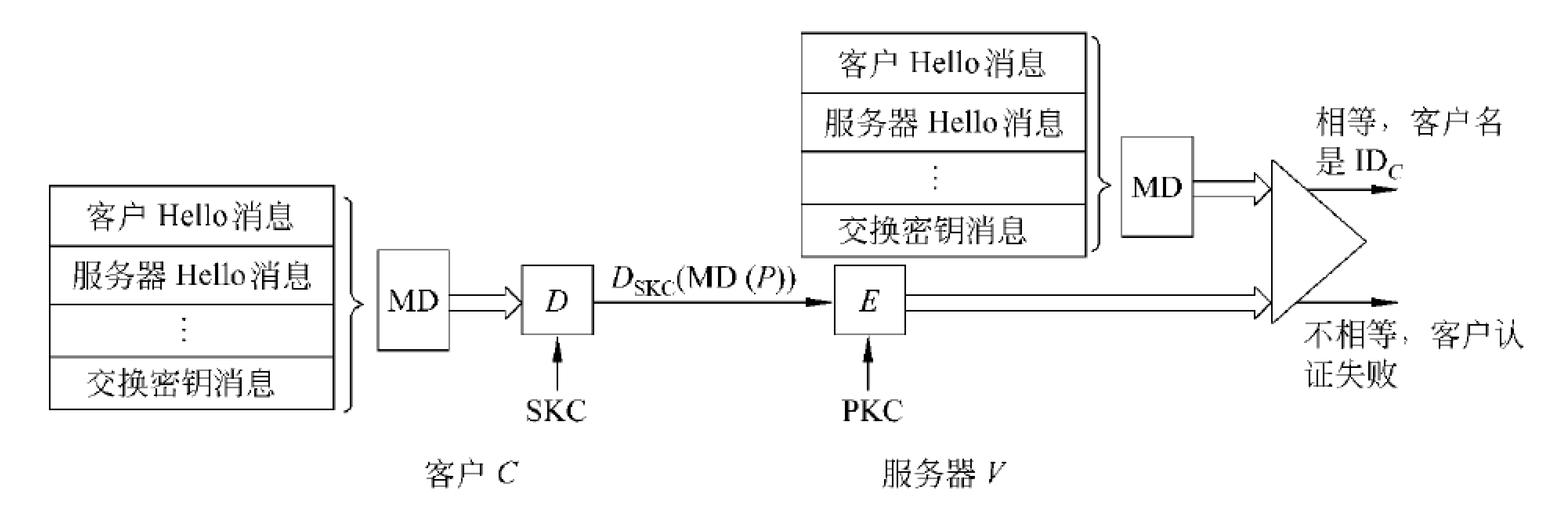


图 3.35　认证客户 C 身份过程

P_hash(密钥,种子)=HMAC-hash(密钥,$A(1)$ ‖ 种子) ‖
HMAC-hash(密钥,$A(2)$ ‖ 种子) ‖
HMAC-hash(密钥,$A(3)$ ‖ 种子) ‖ …

其中
$A(0)$=种子
$A(i)$=HMAC_hash(密钥,$A(i-1)$)

hash 指报文摘要算法,可以是 MD5,或者 SHA-1,因此,P_MD5=HMAC-MD5,P_SHA-1=HMAC-SHA-1,种子是进行报文摘要运算的任意长度的字节流。函数 P_hash的计算过程如图 3.36 所示,每执行 HMAC-hash 一次,产生 128 位(HMAC-MD5)或 160 位(HMAC-SHA-1)输出,重复执行 HMAC-hash 的次数取决于要求输出的结果的

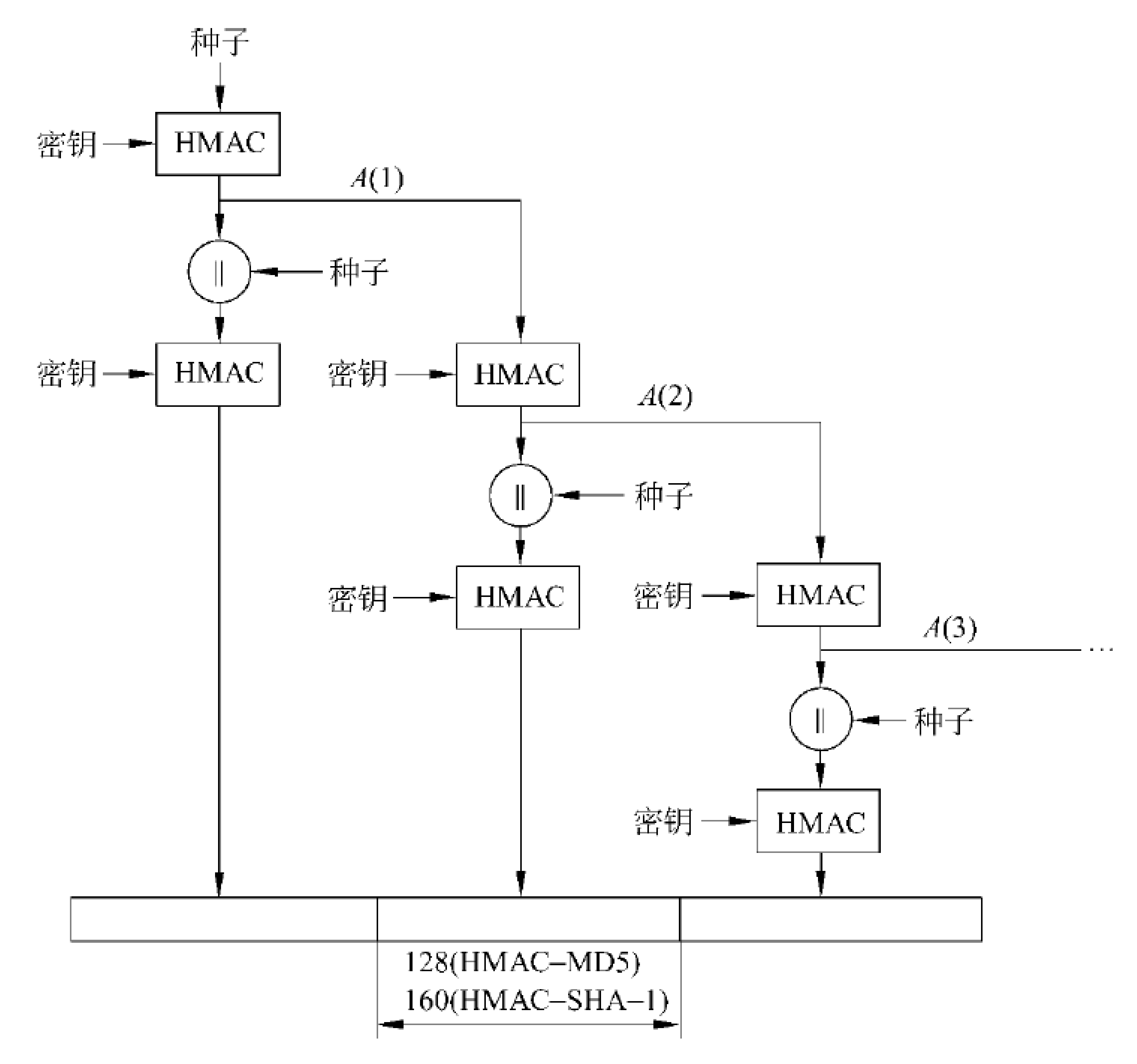


图 3.36　函数 P_hash 计算过程

位数,如果要求最终输出 80 字节的结果,则 HMAC-MD5 需要重复执行 5 次,而 HMAC-SHA-1 需要重复执行 4 次。

PRF(密钥,标签,种子)=P_MD5(S_1,标签 ‖ 种子)⊕P_SHA-1(S_2,标签 ‖ 种子)

其中,PRF 是伪随机数生成函数,S_1 和 S_2 是平分密钥后得到的前半部分和后半部分,标签是任意字符串。P_MD5 为了得到和 P_SHA-1 同样长度的输出结果,必须比 P_SHA-1重复计算更多次。

现在可以得出主密钥计算公式:MK=PRF(PMK,“master secret”,Nonce*C* ‖ Nonce*V*)

这里密钥是预主密钥 PMK,标签是字符串“master secret”,种子是客户随机数 Nonce*C* 和服务器随机数 Nonce*V* 串接在一起的结果。

要证明服务器 *V* 拥有和公钥 PKV 对应的私钥 SKV,只需证明服务器 *V* 得到了预主密钥 PMK。要证明服务器 *V* 得到了预主密钥 PMK,只需证明服务器 *V* 计算所得的主密钥 MK 和客户 *C* 计算所得的主密钥 MK 相同。因此,服务器 *V* 向客户 *C* 发送的结束消息中包含 PRF(MK,“server finished”,MD5(握手协议消息) ‖ SHA-1(握手协议消息))计算结果,客户 *C* 根据自己计算所得的主密钥 MK 重新计算 PRF(MK,“server finished”,MD5(握手协议消息) ‖ SHA-1(握手协议消息)),如果计算结果和服务器 *V* 发送的结束消息中包含的结果相同,服务器 *V* 的身份得到认证。切换安全参数消息表明发送端已经准备开始使用协商所得的安全参数。

TLS 的主要作用是实现服务器的身份认证并生成数据安全传输所需要的安全参数,当然,也可用于实现客户的身份认证,在由服务器对客户进行身份认证时,服务器需要建立授权客户列表,并因此验证客户访问的合法性。

3.4.3 EAP 和 802.1X

在讨论 TLS 协议结构时已经讲过,用 TCP 传输 TLS 记录协议报文的原因是客户和服务器分别是连接在互联网相隔多个传输网络的两端,需要用 IP 实现端到端传输,但许多需要进行身份认证的应用环境并非如此,如无线局域网中 AP 和移动终端之间进行的认证过程,这些应用环境中被认证的用户和认证者往往连接在同一个传输网络中,而且,在完成身份认证前,用户终端并没有分配 IP 地址,因此,也无法用 IP 分组或基于 IP 的运输层协议传输认证协议消息,这些应用环境需要开发基于链路层协议的认证协议,即以传输网络对应的链路层协议为载体协议的认证协议。最容易想到的方法是为每一种被认证用户和认证者连接在同一传输网络上的应用环境建立认证协议和对应的链路层协议之间的绑定关系,如图 3.37 所示。但问题是随着认证协议的独立发展和应用环境的不断增

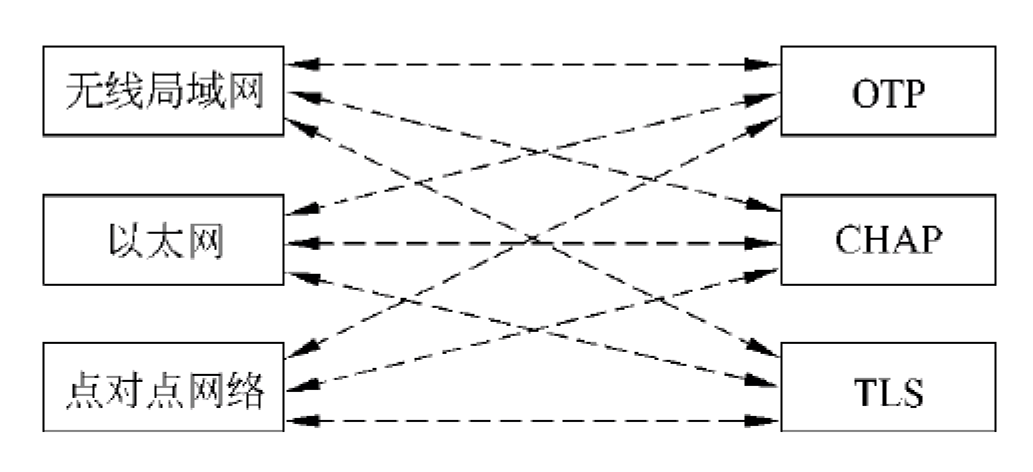


图 3.37 认证协议和应用环境之间的绑定关系

多，这种绑定关系会越来越复杂。如多个属于不同语系的人员如果需要两两之间交换信息，采用图 3.28(a)所示的方式虽然直接，但比较复杂，实际实现过程中往往采用图 3.38(b)所示的方式，选择其中一种语言作为交流语言，其他所有语言先翻译成交流语言，再和不同语系的人员交流，这样，所有不同语系的人员只要能够实现和交流语言的相互转换，就能和其他语系的人员进行交流。同样，认证协议和应用环境之间也不会采用两两之间相互绑定的方式，而是先定义一种和应用环境无关的、用于传输认证协议消息的载体协议，所有应用环境和认证协议都和这种载体协议绑定，如图 3.39 所示。这样，每出现新的应用环境，建立该应用环境和载体协议之间的绑定，每发展出新的认证协议，建立该认证协议和载体协议之间的绑定。这种载体协议就是扩展认证协议(Extensible Authentication Protocol，EAP)。为了便于区分，把和 EAP 绑定的认证协议称为认证机制。

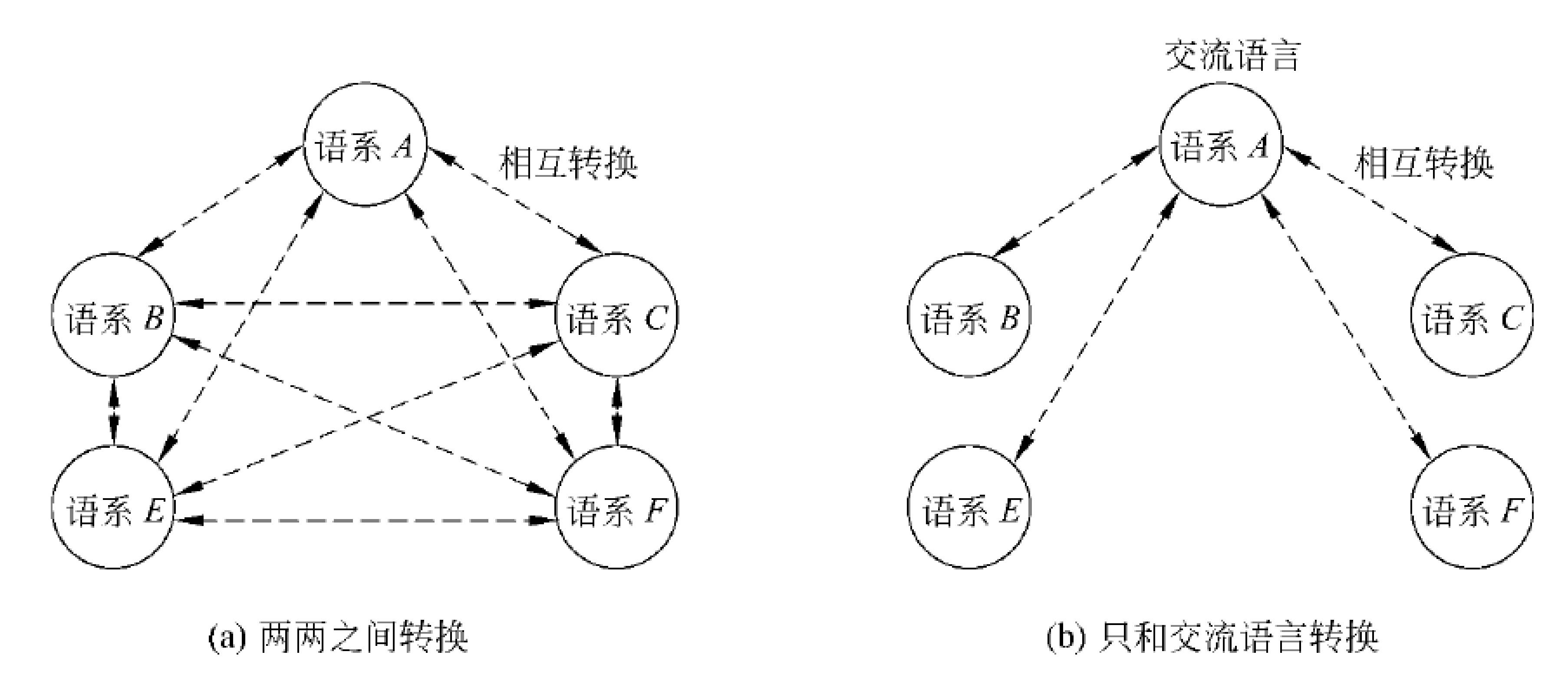


图 3.38 多种语系人员交换信息方式

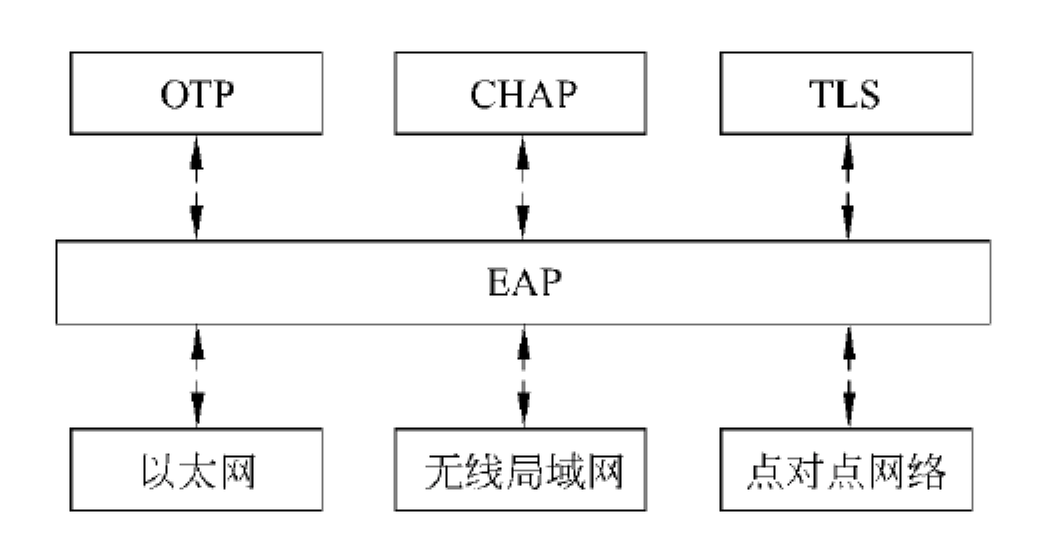


图 3.39 EAP 的作用和地位

1. EAP 操作过程

EAP 的操作模型如图 3.40 所示，认证者负责对用户进行认证，用户只有通过认证者的认证才能接入，因此，在接入网络中，终端用户就是图 3.40 中的用户，网络接入服务器(远程用户接入设备或宽带接入服务器)就是图 3.40 中的认证者。认证者向用户发送请求报文，用户向认证者回送响应报文。请求报文和响应报文的内容与双方采用的认证机制有关，不同的认证机制有着不同的请求/响应过程，有的认证机制可能需要经过多次请求/响应过程才能完成用户认证。如果请求/响应过程按照认证机制操作规则正常完成，

认证者向用户发送成功报文,表示成功完成用户认证。否则,向用户发送失败报文,表示认证失败。

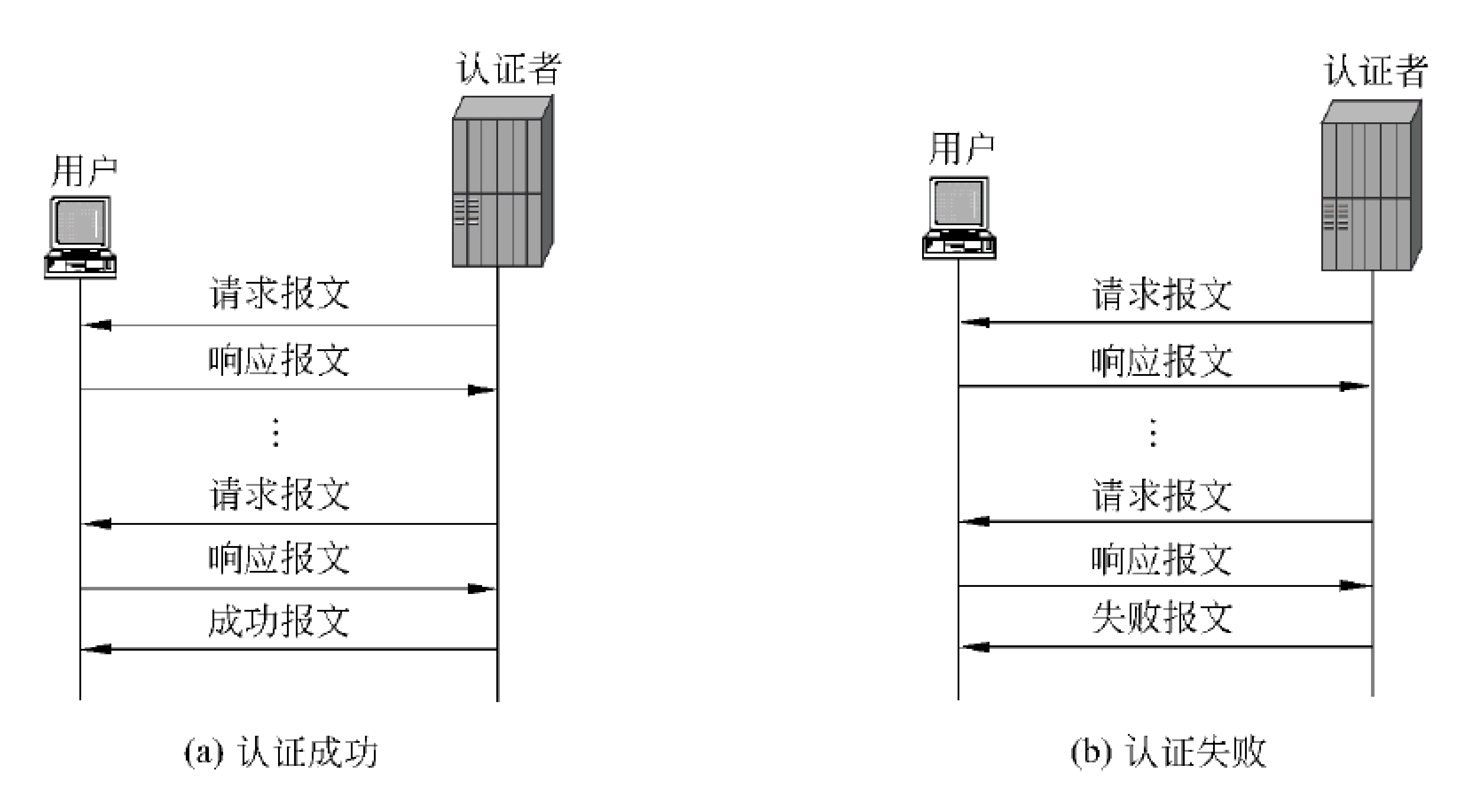


图 3.40 EAP 操作模型

EAP 报文格式如图 3.41 所示,编码字段给出报文的类型,EAP 共定义了四种类型的报文,它们分别是请求、响应、成功和失败报文,对应的编码分别是 1～4。标识符字段用来匹配请求和响应报文,EAP 必须在上一次请求/响应过程完成后,才能开始下一次请求/响应过程,每一次请求/响应过程中,请求报文和响应报文必须具有相同的标识符。认证者发送请求报文后,等待用户发送响应报文,如果经过规定时间仍未接收到响应报文,就向用户重发请求报文,重发的请求报文维持标识符不变。用户接收到请求报文后,必须回送对应的响应报文,如果接收到具有和前一个请求报文相同标识符的请求报文,用户认为接收到了重复的请求报文,将丢弃该请求报文,并重发前一个请求报文对应的响应报文。同样,当认证者接收到两个标识符相同的响应报文时,认为重复接收了响应报文,将丢弃第 2 个响应报文。因此,相邻两次请求/响应过程必须采用不同的标识符。长度字段给出 EAP 报文总的长度。只有请求/响应报文才包含数据字段,数据字段的第 1 个字节是类型字段,给出数据类型,一般情况下,请求/响应报文数据字段所包含的数据类型与采用的认证机制有关,因此,数据字段的第 1 个字节常用来指定所采用的认证机制。类型为身份的请求/响应过程用来确定用户和认证者的身份,由于不同用户可能采用不同的认证机制,因此,需要在开始认证过程前,确定用户身份,然后,选择对应的认证机制认证用户身份。

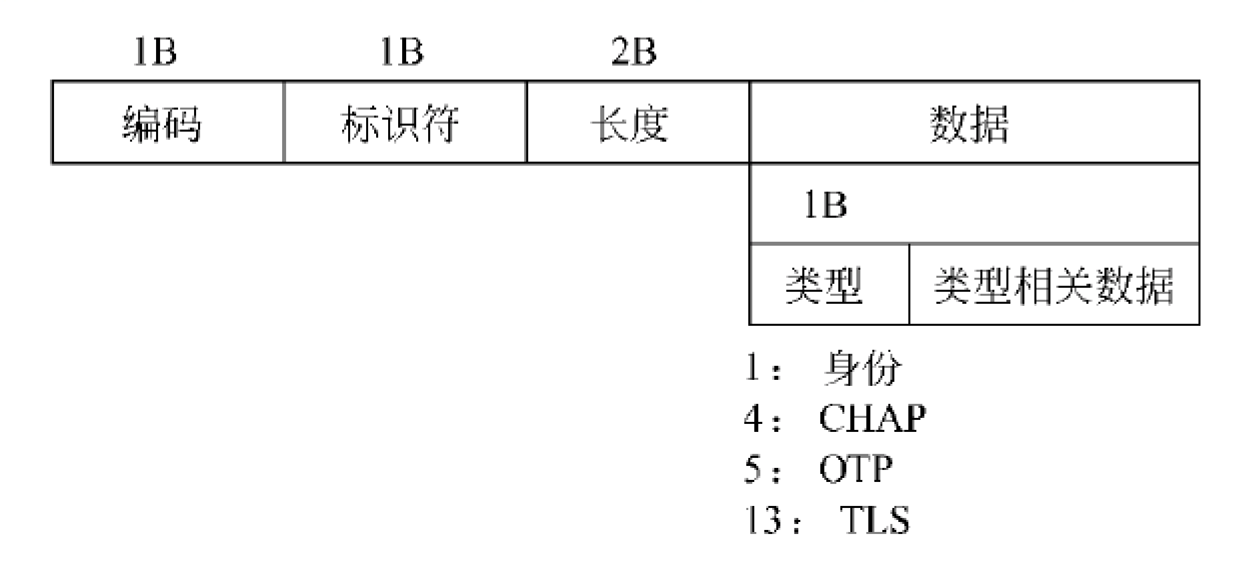


图 3.41 EAP 报文格式

2. EAP over PPP

点对点协议(Point-to-Point Protocol,PPP)是点对点网络,如 PSTN,对应的链路层协议,自然也是点对点网络环境下的 EAP 载体协议,用于实现用户和认证者之间的 EAP 报文传输。为了用 PPP 传输 EAP 报文,在 PPP 通过 LCP 建立 PPP 链路时,在配置项中约定双方使用的认证协议是 EAP。PPP 封装 EAP 报文的过程如图 3.42 所示。如果认证服务器通过配置,对拨号上网用户采用挑战握手认证协议(Challenge Handshake Authentication Protocol,CHAP)作为认证机制,整个认证过程如图 3.43 所示。

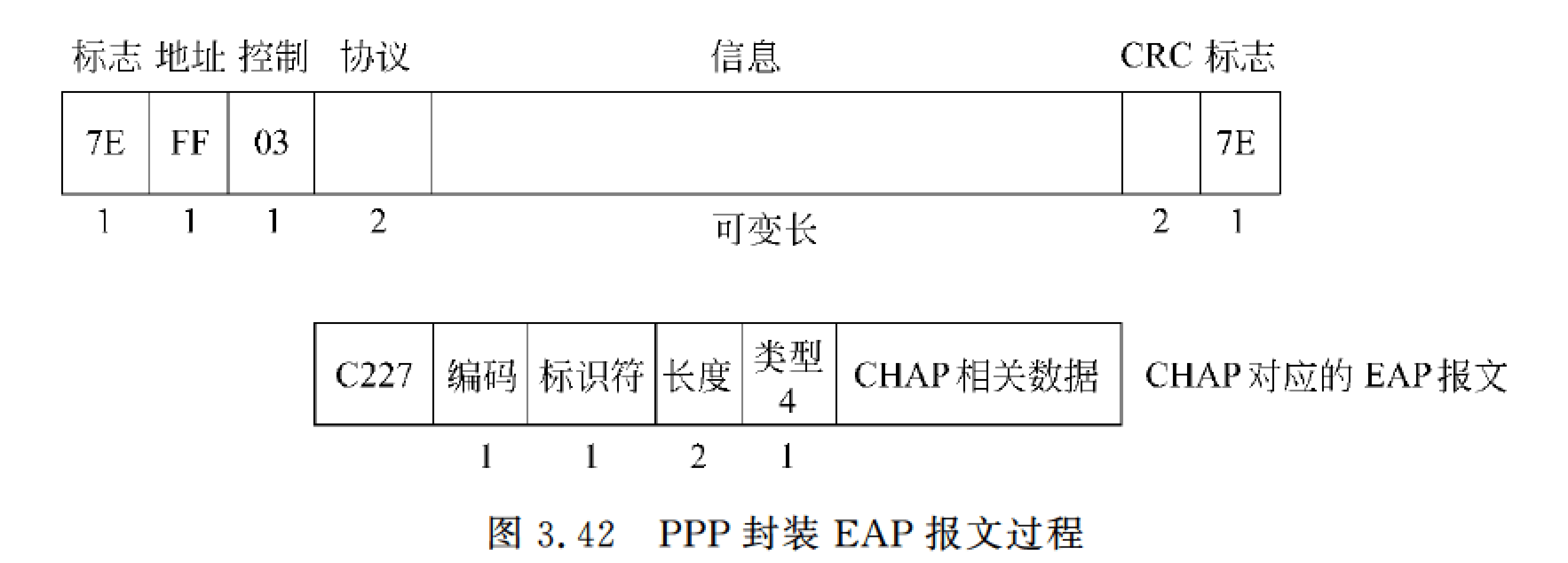


图 3.42　PPP 封装 EAP 报文过程

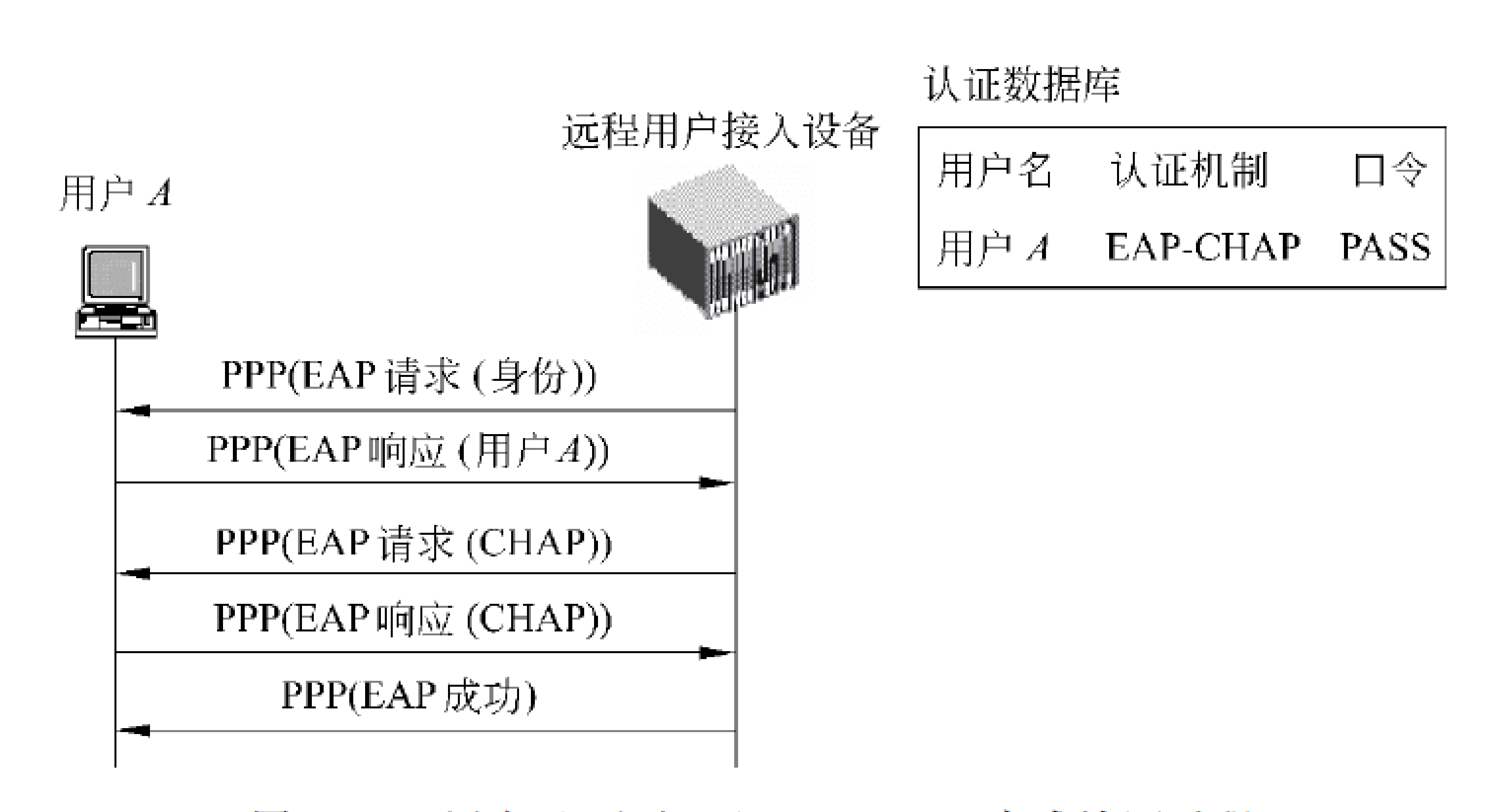


图 3.43　用户 A 通过 EAP over PPP 完成认证过程

图 3.43 中,用户 A 通过呼叫连接建立过程建立和远程用户接入设备之间的语音信道,双方通过传输 LCP 帧建立 PPP 链路,并在建立 PPP 链路过程中约定采用 EAP 作为认证协议。在成功建立 PPP 链路后,远程用户接入设备作为认证者向用户 A 发出 EAP 请求报文,要求用户 A 提供用户名。用户 A 通过 EAP 响应报文向远程用户接入设备提供用户名:用户 A。当然,双方交换的 EAP 报文均按照图 3.42 所示的封装过程封装成 PPP 帧后进行传输。当远程用户接入设备接收到用户 A 回送的 EAP 响应报文,用用户名检索认证数据库,确定该用户是否是注册用户,注册时配置的认证机制和口令。在确定用户 A 关联的认证机制和口令后,根据 CHAP 的认证操作过程,向用户 A 发送随机数 challenge。远程用户接入设备根据认证机制 CHAP 对应的数据类型(类型 4)将随机数 challenge 封装成 EAP 请求报文,并将 EAP 请求报文按照图 3.42 所示的封装过程封装成 PPP 帧后,通过语音信道传输给用户 A。用户 A 根据 CHAP 认证操作过程,将请求报

文的标识符字段值、challenge 和口令串接在一起，并对串接操作后的结果进行 MD5 报文摘要运算(MD5(标识符 ‖ challenge ‖ 口令))，并通过 EAP 响应报文将运算结果回送给远程用户接入设备。远程用户接入设备重新对保留的标识符字段值、challenge 和认证数据库中用户 *A* 关联的口令进行上述运算((MD5(标识符 ‖ challenge ‖ 口令))，并将计算所得的结果和 EAP 响应报文中给出的结果比较，如果相同，向用户 *A* 发送认证成功报文，否则，向用户 *A* 发送认证失败报文。

3. 802.1X 操作过程

链路层认证机制的目的和应用层认证机制的目的不同，应用层认证机制在完成对客户的身份认证后，必须产生用于证明后续服务请求是已认证用户所发送的安全参数，如加密密钥、MAC 密钥等，客户在以后发送的服务请求中必须通过这些安全参数证明发送者身份。由于一些传输网络中，用户和连接用户的物理链路或逻辑链路是一一对应的，因此，对链路层认证机制的认证者而言，认证过程就是确定连接用户的物理或逻辑链路的有效性的过程，如对拨号上网用户的认证过程就是确定远程用户接入设备和终端之间语音信道的有效性的过程，认证成功，该物理链路有效，远程用户接入设备可以转发从该物理链路输入输出的数据。同样，对于用基于以太网的 PPP(PPP over Ethernet，PPPOE)实现以太网接入的用户，认证成功，表示终端和宽带接入服务器之间的 PPP 会话有效，宽带接入服务器可以转发从该 PPP 会话输入输出的数据。802.1X 是基于端口的接入控制协议，它的目的在于通过认证过程确定连接终端的端口是否有效，该端口有效，表示以太网交换机可以转发从该端口输入输出的数据。

802.1X 通过 EAP 完成对接入用户的认证过程。EAP 报文封装成 LAN 对应的帧格式在用户和认证者之间相互传输，EAP over LAN(EAPOL)给出了将 EAP 报文封装成 LAN 对应的帧格式的过程。目前支持 802.1X 的局域网主要是以太网和无线局域网，这里主要讨论以太网环境中 802.1X 的操作过程，第 5 章讨论无线局域网环境中 802.1X 的操作过程。

802.1X 的操作模型如图 3.44 所示，一个物理端口被虚化成两个虚端口，一个是受控端口，只有在通过认证后，才能提供正常的输入输出服务；另一个是非受控端口，用于接收 EAP 报文和其他广播报文。以太网交换机作为认证者或者直接完成对用户的认证，或者作为中继系统，在用户和认证服务器之间转发 EAP 报文。受控端口在完成用户认证前，处于非授权状态，不能输入输出数据帧，只有通过对接入端口的用户的身份认证后，才能从非授

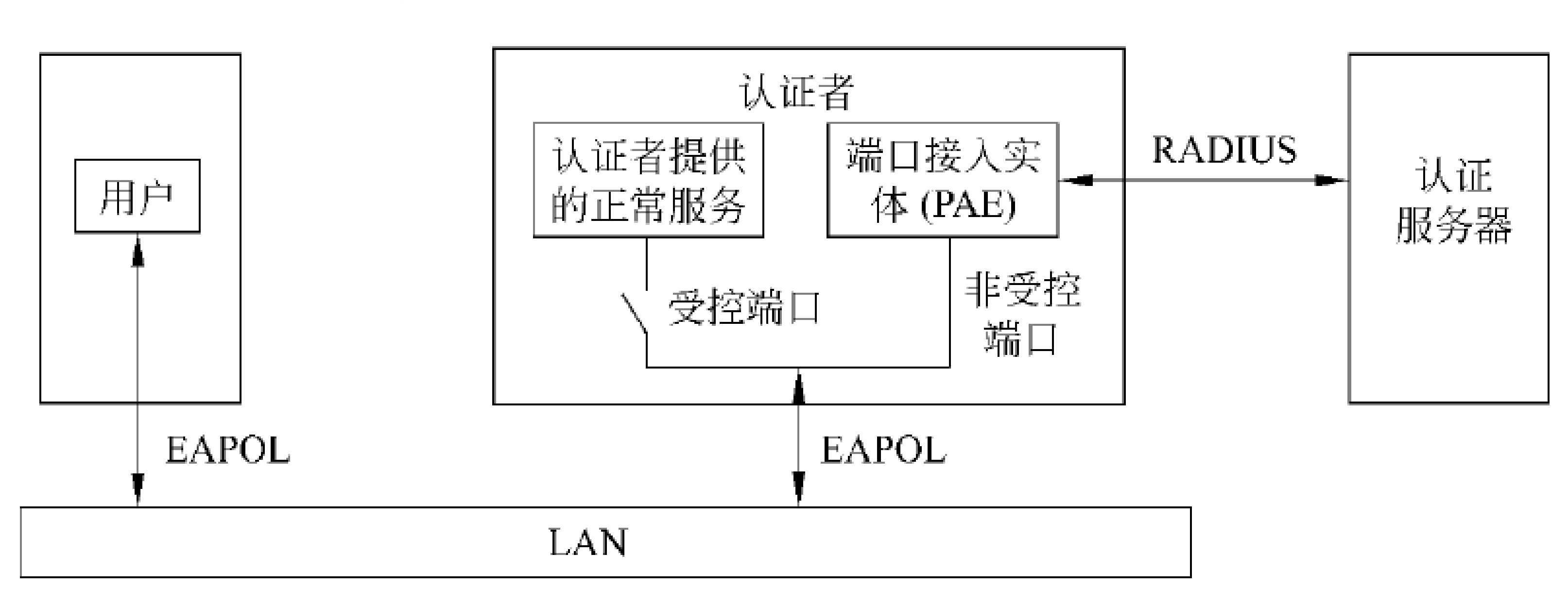


图 3.44　802.1X 操作模型

权状态转变为授权状态。用户通过下线或退出操作将受控端口从授权状态转变为非授权状态。非受控端口一直允许接收 EAP 报文,并将接收到的 EAP 报文提交给端口接入实体(Port Access Entity,PAE),由 PAE 根据认证者的功能配置,或直接进行认证操作或转发 EAP 报文。非受控端口的这种工作状态不受认证过程的影响。这意味着一旦以太网交换机的某个端口被启动 802.1X 认证功能,在通过对接入用户的认证前,该端口只能输入输出 EAP 报文和广播帧,只有通过对接入端口的用户的认证后,该端口才能正常输入输出数据帧。

EAPOL 封装格式如图 3.45 所示,版本字段值目前固定为 2,报文类型表明封装在 MAC 帧中的报文类型,目前定义了五种报文类型,见表 3.2。报文体长度和报文体由报文类型决定。

6B	6B	2B	1B	1B	2B		4B
目的地址	源地址	类型:888E	版本	报文类型	报文体长度	报文体	FCS

图 3.45　EAPOL 封装格式

表 3.2　EAPOL 报文类型

报文类型字段值	报 文 类 型	描　　述
0	EAP 报文	报文体为 EAP 报文
1	EAPOL-Start	认证发起报文,用于由用户发起的认证过程
2	EAPOL-Logoff	退出报文,用于退出端口的授权状态
3	EAPOL-Key	密钥报文,用于交换密钥,用于无线局域网
4	EAPOL-ASF-Alert	报警报文,当受控端口处于非授权状态时,用于交换机接收报警消息

图 3.46 和图 3.43 基本相同,只是一是由 EAP over PPP 变为 EAP over LAN,二是由用户通过向认证者发送 EAPOL-Start 报文发起认证过程。在 802.1X 中,认证者和用户均可发起认证过程,如果由认证者发起认证过程,EAP 报文的传输顺序和图 3.43 相

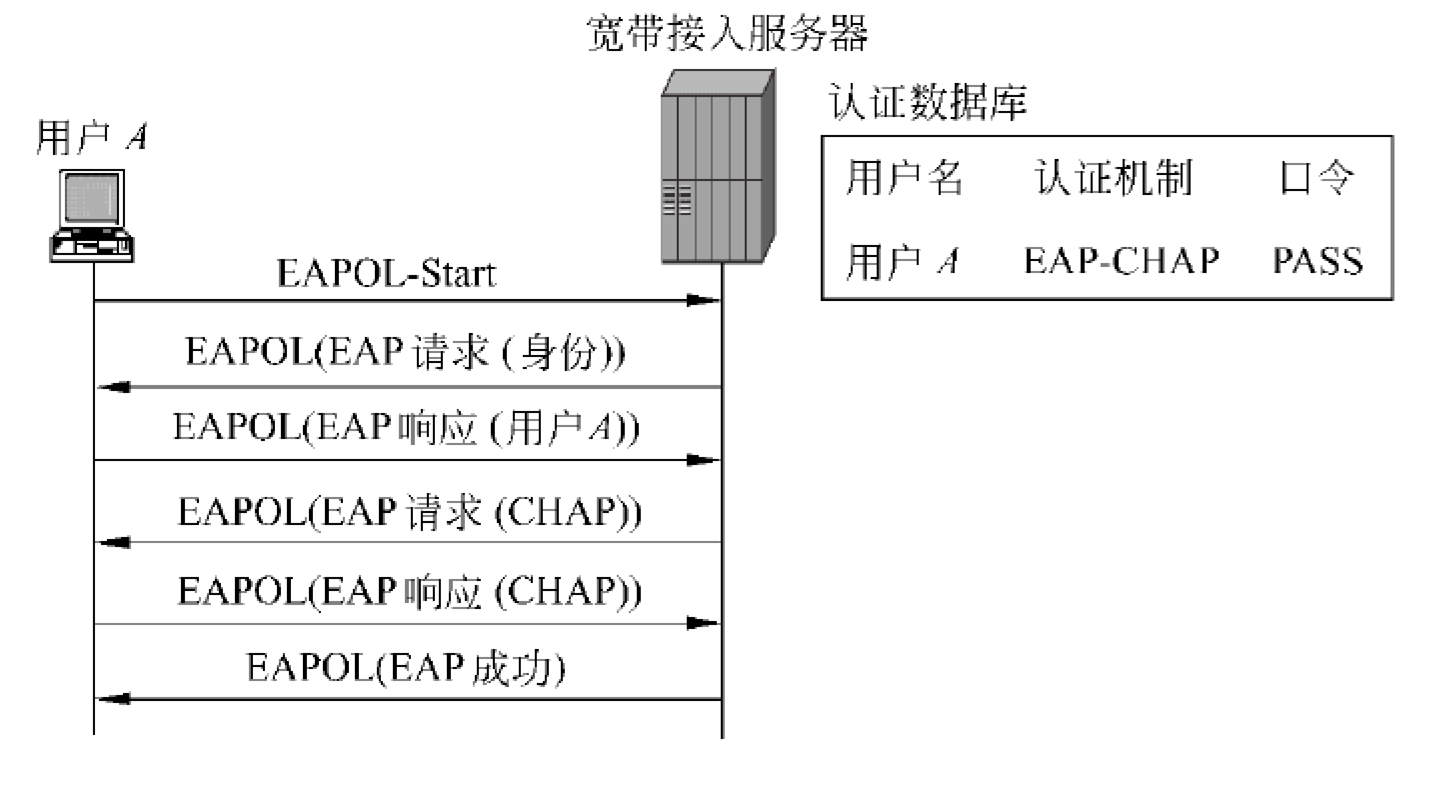


图 3.46　802.1X 认证接入用户过程

同,如果由用户发起认证过程,必须由用户首先向认证者发送 EAPOL-Start,如图 3.46 所示。

由于 802.1X 是基于端口的接入控制协议,对于图 3.47 所示的接入网络结构,一旦宽带接入服务器连接以太网的端口从非授权状态转变为授权状态,所有连接在以太网上的终端均可通过该端口正常转发数据帧,这当然不符合接入控制要求。解决这一问题的方法有两种,一是将 802.1X 的功能配置到接入交换机,如图 3.47 中的楼内交换机;二是改进 802.1X 的接入控制功能。目前以太网交换机实现的 802.1X 都是基于 MAC 地址,而不是基于端口进行接入控制,交换机每一个端口都配置访问控制列表,只有源 MAC 地址在端口的访问列表中且对应的访问控制是允许访问时,该 MAC 帧才能通过受控端口进行转发。当某个用户希望接入 Internet 时,通过发送 EAPOL-Start 发起认证过程。一旦通过认证,将该终端的 MAC 地址列入接收到 EAP 报文的端口对应的访问控制列表,并将访问控制设置为允许访问,以后,所有以该 MAC 地址为源 MAC 地址的 MAC 帧进入该端口后,均能予以正常转发。

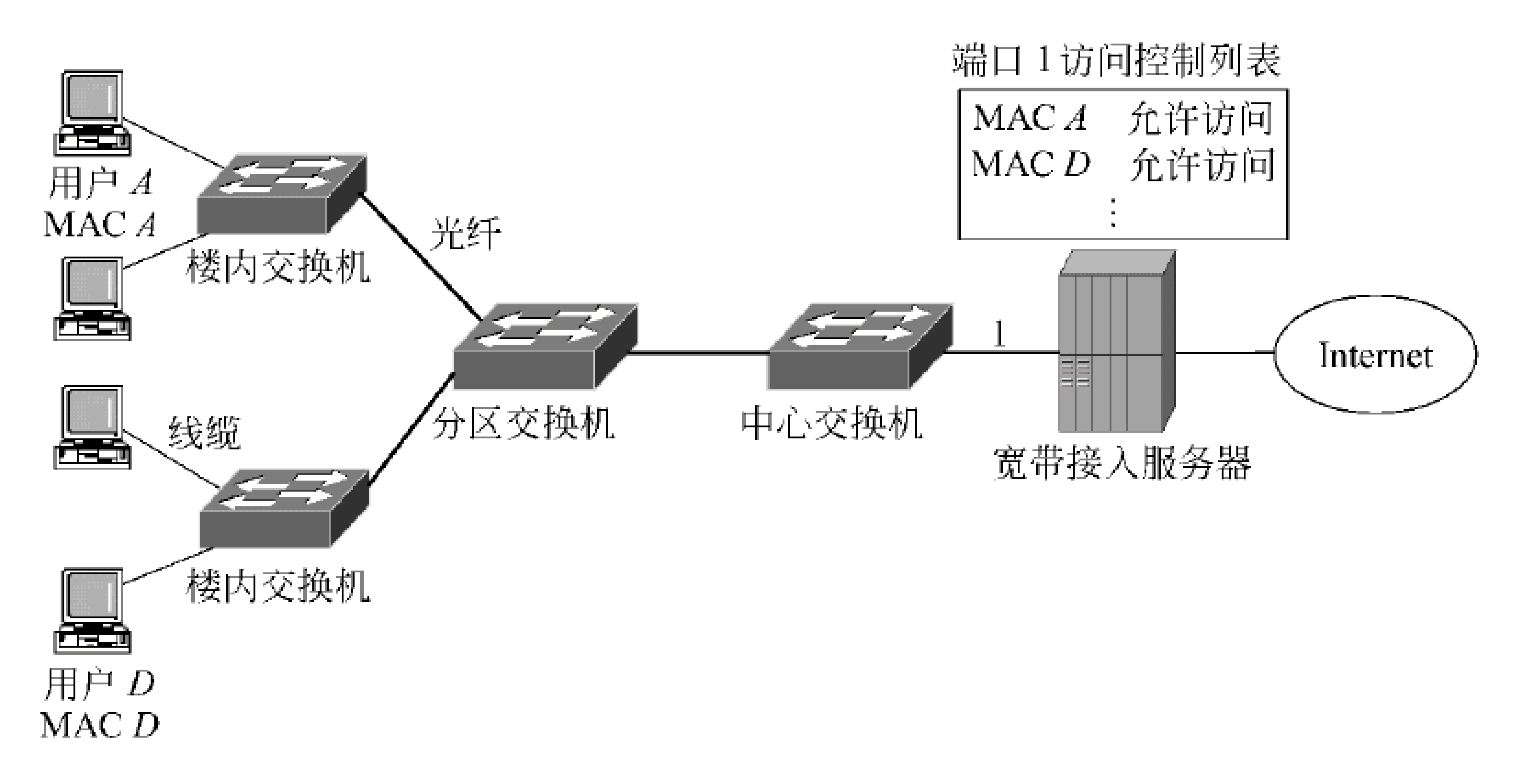


图 3.47 以太网作为接入网络的网络结构

当用户发送 EAPOL-Start 时,往往不知道宽带接入服务器连接以太网的端口的 MAC 地址,因此,固定用组地址 01:80:C2:00:00:03 作为 MAC 帧的目的 MAC 地址,这是分配给 PAE 的组地址,如果某个端口启用了 802.1X 功能,该端口将所有以该组地址为目的 MAC 地址的 MAC 帧提交给 PAE 处理,否则,以广播方式转发该 MAC 帧。针对这种转发方式,用于接入网的以太网交换机常常将每一个接入端口和上联端口作为一个广播域,这样,从接入端口输入的广播帧只能通过上联端口转发出去,避免了一个终端发送的广播帧影响另一个终端的情况发生。

3.4.4 RADIUS

1. RADIUS 功能

Internet 服务提供者(Internet Service Provider,ISP)接入网络往往设置多个接入点,提供多种接入方式,如图 3.48 所示,在这种网络结构下,拨号用户和远程用户接入设备之间没有绑定关系。同样,对于图 3.49 所示的无线局域网扩展服务集结构,移动终端和

AP之间也没有绑定关系，因此，用AP或远程用户接入设备作为认证者用于完成对接入用户的认证是比较困难的。另外，为了便于统一管理，也需要设置认证服务器，由认证服务器统一管理用户，完成对用户的认证、授权和计费操作，如图3.48和图3.49所示，这种情况下，认证者不再进行具体的认证操作，它只作为中继系统，向认证服务器转发用户发送的响应报文，或向用户转发认证服务器发送的请求报文。为了完成认证者和认证服务器之间的EAP报文传输，必须定义一种载体协议。需要强调的是用户和认证者之间和认证者和认证服务器之间用于传输EAP报文的载体协议是不同的，这主要因为，对于前者，一方面，在完成对用户的认证过程前，用户通常不具有IP地址。另一方面，用户和认证者之间的接入网络或是单一类型的传输网络，如PSTN和以太网，可以直接通过链路层传输路径完成用户和认证者之间的EAP报文传输。或是虽然由多个不同类型的传输网络组成，但用隧道方式在用户和认证者之间建立跨多个传输网络的链路层传输路径，用户和认证者之间仍然可以通过链路层传输路径完成EAP报文传输，如ADSL。因此，用户和认证者之间的载体协议通常是和传输网络对应的链路层协议。但认证者和认证服务器之间的传输通路往往是由路由器互连的多段链路层传输路径组成的，因此，必须用IP以上的协议作为载体协议，远程认证拨入用户服务(Remote Authentication Dial In User Service，RADIUS)就是这样一种基于IP的载体协议。

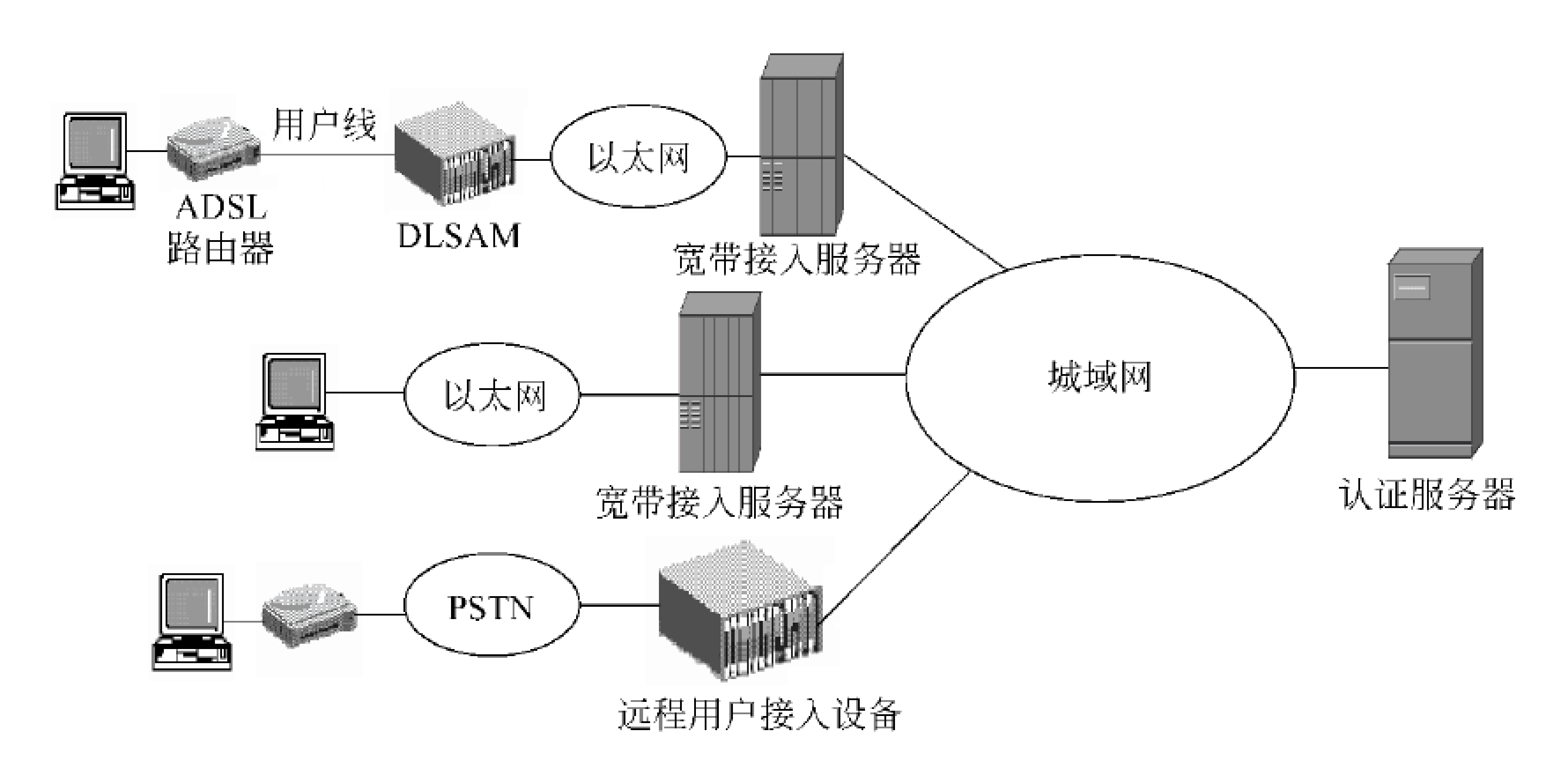


图3.48　ISP接入网络结构

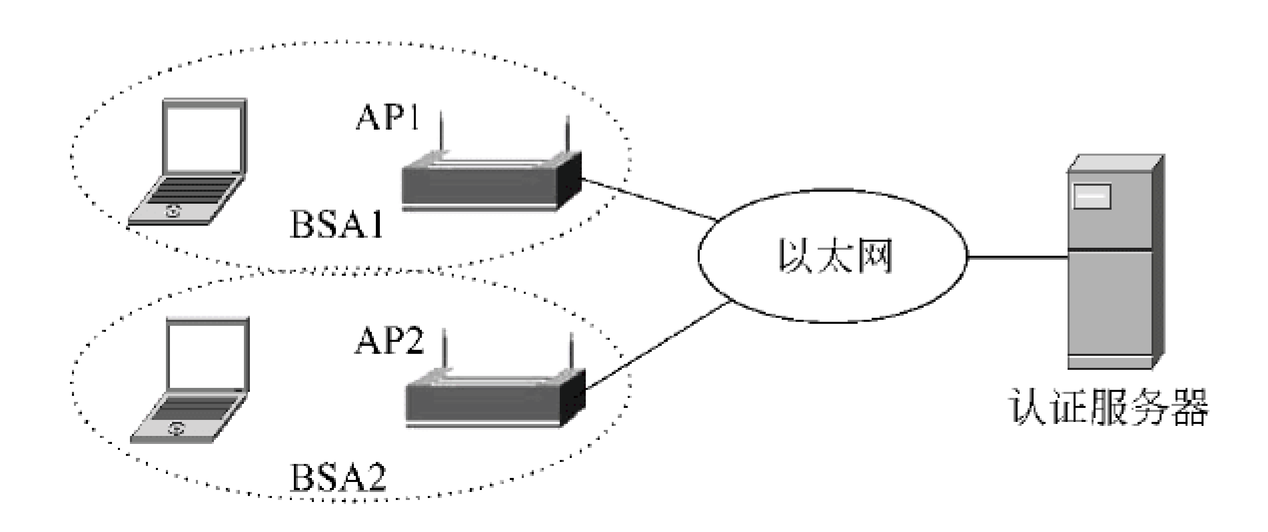


图3.49　无线局域网扩展服务集结构

2. RADIUS 报文格式

RADIUS 属于应用层协议，因此，RADIUS 报文先封装成运输层报文，然后，再把运输层报文封装成 IP 分组，用于传输 RADIUS 报文的运输层协议是 UDP，封装过程如图 3.50所示。

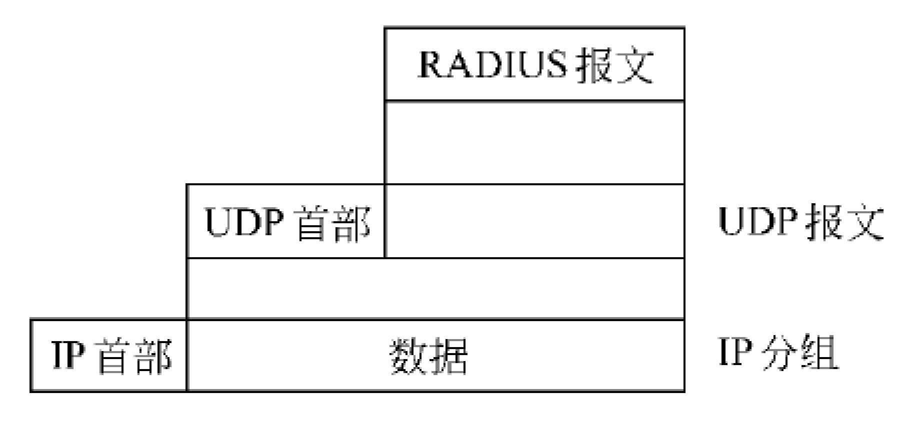


图 3.50 封装 RADIUS 报文过程

RADIUS 报文格式如图 3.51 所示，编码字段给出 RADIUS 报文类型，目前主要定义了四种 RADIUS 报文，它们分别是请求接入、允许接入、拒绝接入和挑战接入报文，请求接入报文用于传输用户提供的认证信息，如用户名、口令等，允许接入报文表明认证服务器完成对用户的认证，允许用户接入网络。拒绝接入报文表明用户提供的认证信息无法使认证服务器完成对用户的认证，拒绝用户接入网络，挑战接入报文或者需要用户通过请求接入报文提供更多的认证信息，或者需要用户根据约定的认证机制对挑战接入报文中包含的数据进行运算，并将运算结果通过请求接入报文提供给认证服务器，根据所使用的认证机制，用户和认证服务器之间可能需要交换多对挑战接入和请求接入报文。认证过程中交换 RADIUS 报文的过程如图 3.52 所示。认证服务器用于认证用户的信息来自用户，但通常情况下，由基于链路层的认证协议完成用户和认证者之间的传输过程，由 RADIUS 完成认证者和认证服务器之间的传输过程，在 RADIUS 中，用于在用户和认证服务器之间起中继作用的认证者称为网络接入服务器(Network Access Server，NAS)。



1. 请求接入
2. 允许接入
3. 拒绝接入
11. 挑战接入

图 3.51 RADIUS 报文格式

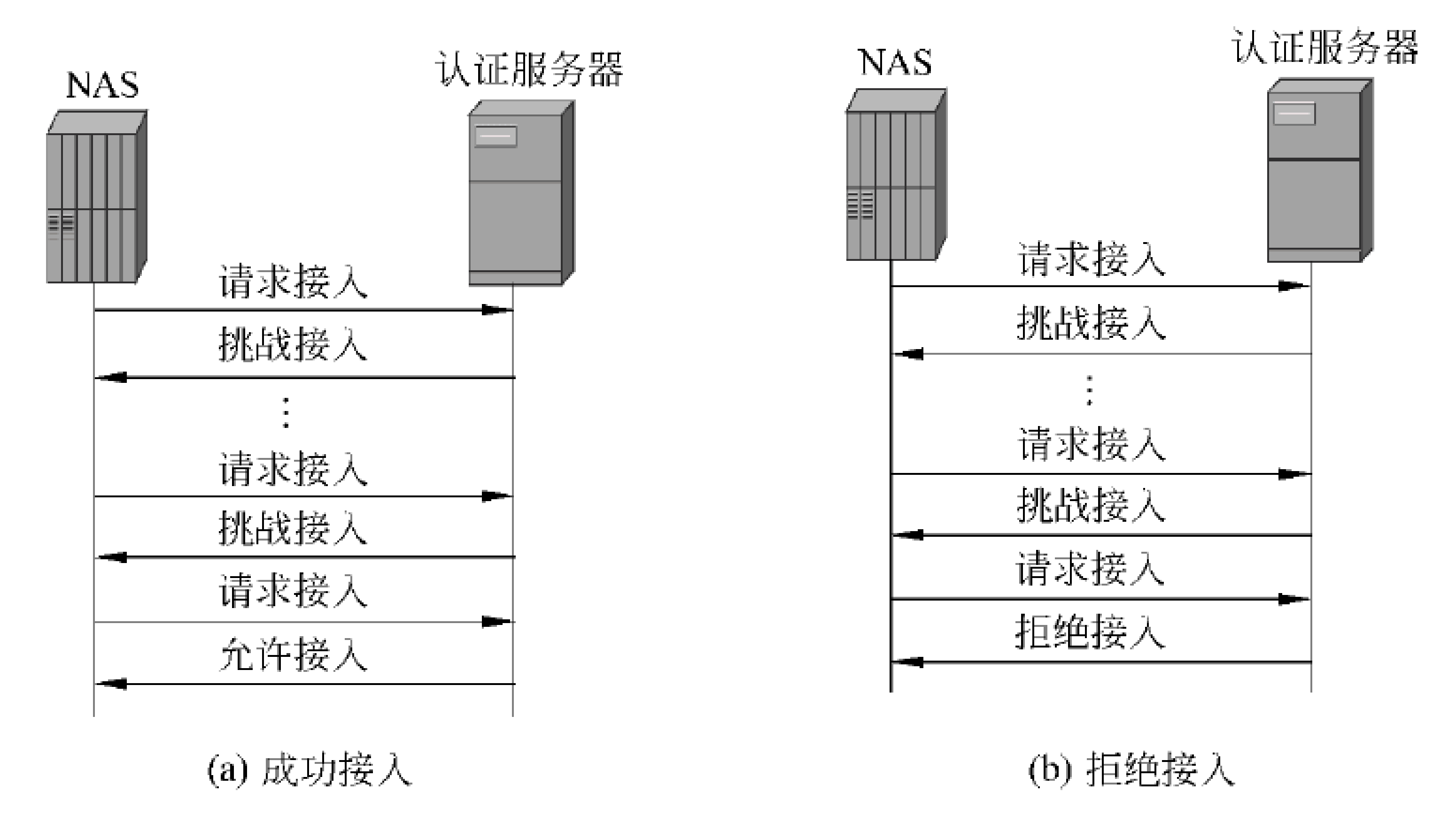


图 3.52 RADIUS 报文交换过程

标识符字段用于匹配请求接入报文和对应的响应报文，如允许接入报文、挑战接入报文或拒绝接入报文，每一个请求接入报文选择不同的标识符，对应的响应报文的标识符必须和请求接入报文的标识符相同，NAS 以此确定和该响应报文匹配的请求接入报文。

长度字段给出 RADIUS 报文的总长。

认证信息字段用于认证发送响应报文的认证服务器，NAS 和认证服务器之间必须约定一个共享密钥 K，双方通过共享密钥 K 加密敏感信息，如用户口令等，同时 NAS 通过共享密钥 K 完成对认证服务器的认证，防止黑客仿冒认证服务器窃取用户信息。请求接入报文中的认证信息是一个 16 字节的随机数，为了防止中继攻击，在 NAS 和认证服务器之间的共享密钥有效期内，不允许在请求接入的报文中出现相同的随机数，即认证信息。认证服务器发送的响应报文，如允许接入、拒绝接入和挑战接入报文中的认证信息通过下式计算所得：

响应报文认证信息＝MD5（响应报文 ‖ 对应请求接入报文的认证信息 ‖ 共享密钥）

响应报文指除认证信息字段外的所有其他字段信息，包括编码、标识符、长度和所有属性字段。

属性字段给出用户信息和 NAS 信息，如用户名、口令、NAS 标识符、NAS IP 地址，认证服务器根据用户信息完成对用户的认证，根据 NAS 信息确定共享密钥，RADIUS 支持常见的认证机制，如 PAP、CHAP，定义了和这些认证机制相关的属性。RADIUS 作为承载协议，属性类型和数据格式与采用的认证机制密切相关，因而需要随着认证机制的发展不断定义新的属性，目前，EAP 的性质和 RADIUS 相似，只是 EAP 基于链路层，适用于由单一传输网络组成的应用环境，而 RADIUS 基于 IP，适用于由多种不同类型传输网络互联而成的应用环境，为了避免重复劳动，EAP 不断增加和新发展的认证机制相匹配的数据类型，但在 RADIUS 中只增加用于封装 EAP 报文的 EAP 属性，这样，和新发展的认证机制相关的数据类型和格式先封装成 EAP 报文，然后，将 EAP 报文封装成 RADIUS 的 EAP 属性，通过 RADIUS 报文实现 NAS 和认证服务器之间的 EAP 报文传输。

有关用户敏感信息的属性，如用户口令，需要进行加密操作，加密运算过程如下：第一步将用户口令分成 16 字节长度的数据块 P_i，不足 16 字节或不是 16 字节整数倍的用户口令通过填充使其长度成为 16 字节的整数倍。第二步实现加密运算。

$$B_1 = \text{MD5}(\text{认证信息} \parallel \text{共享密钥}), \quad C_1 = B_1 \oplus P_1$$

$$B_2 = \text{MD5}(C_1 \parallel \text{共享密钥}), \quad C_2 = B_2 \oplus P_2$$

$$\vdots$$

$$B_i = \text{MD5}(C_{i-1} \parallel \text{共享密钥}), \quad C_i = B_i \oplus P_i$$

$$\text{用户口令属性值} = C_1 \parallel C_2 \parallel \cdots \parallel C_i$$

3. RADIUS 应用

用户、认证者（NAS）和认证服务器协调完成认证的操作过程如图 3.53 所示。当用户 C 和 NAS 之间建立物理连接，NAS 向用户 C 发送 EAP 请求报文，要求用户 C 提供用户名。用户 C 通过 EAP 响应报文向 NAS 提供用户名用户 C。当然，双方交换的 EAP 报文均封装成互联 NAS 和用户 C 的传输网络对应的链路层帧格式。NAS 接收到用户 C 发送的 EAP 响应报文后，将 EAP 响应报文作为 RADIUS 报文的 EAP 属性，构成

RADIUS 报文，并通过互联 NAS 和认证服务器的 IP 网络，将 RADIUS 报文传输给认证服务器。当认证服务器接收到用户提供的用户名用户 C，用用户名检索认证数据库，确定该用户是否是注册用户，注册时配置的认证机制和口令。在确定用户 C 关联的认证机制和口令后，根据 CHAP 的认证操作过程，向用户 C 发送随机数 challenge。认证服务器根据认证机制 CHAP 对应的数据类型(类型 4)将随机数 challenge 封装成 EAP 请求报文，并将 EAP 请求报文封装成 RADIUS 报文后，通过 IP 网络传输给 NAS。NAS 将 EAP 请求报文重新封装成互联 NAS 和用户 C 的传输网络对应的链路层帧格式后，传输给用户 C。用户 C 根据 CHAP 认证操作过程，计算 MD5(标识符 ‖ challenge ‖ 口令)，并通过 EAP 响应报文将结果回送给认证服务器。认证服务器重新计算结果，并将计算所得的结果和 EAP 响应报文中给出的结果比较，如果相同，向 NAS 发送允许接入报文；否则，向 NAS 发送拒绝接入报文。NAS 根据认证服务器发送的认证结果，向用户 C 发送认证成功或认证失败报文。

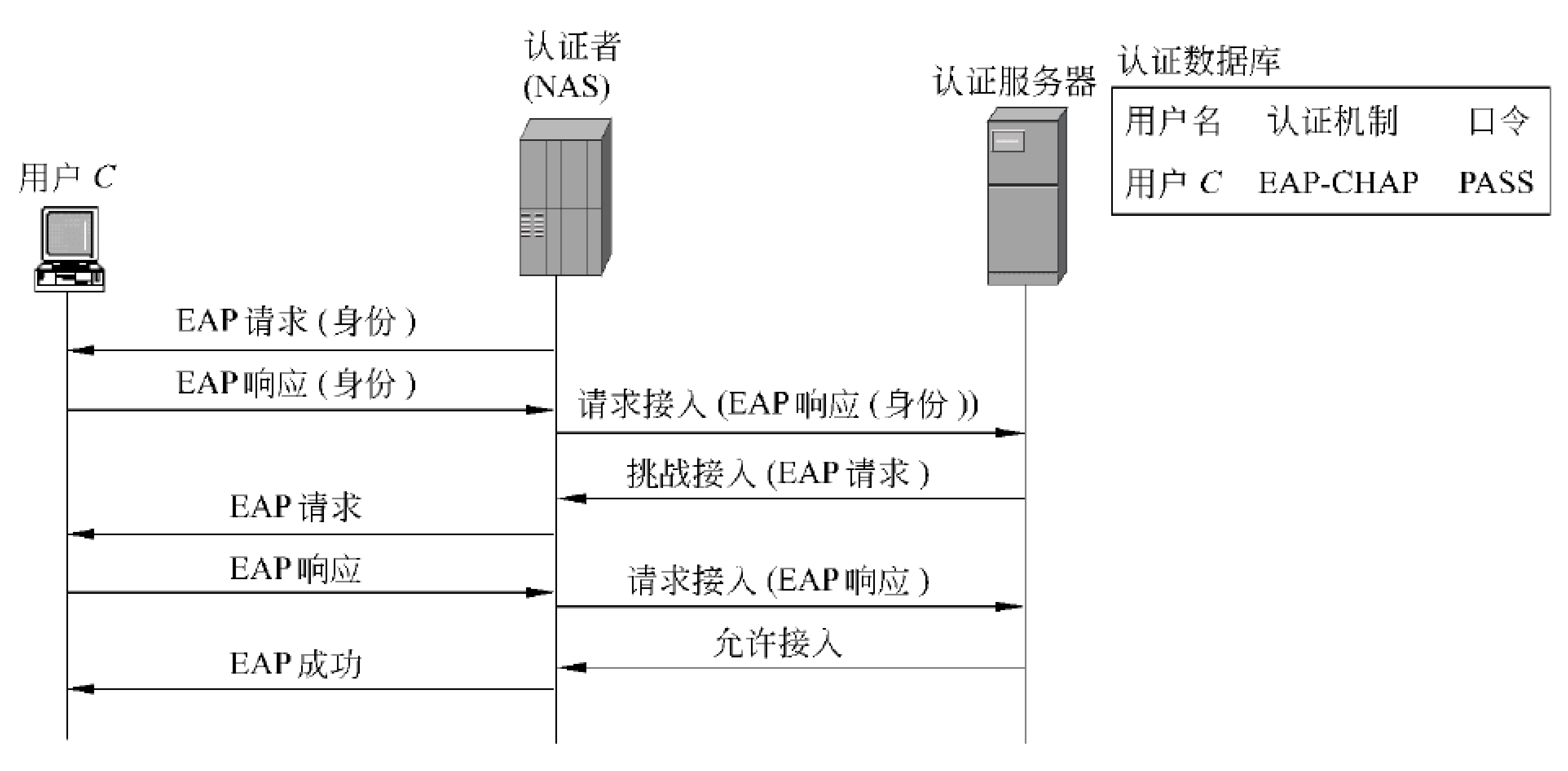


图 3.53 RADIUS 和 EAP 协调完成认证过程

3.5 IPSec

目前，已经有多种针对不同应用的认证协议，如用于 C/S 访问方式的 Kerberos，它由统一的认证服务器完成客户身份认证，由统一的通行证签发服务器完成客户服务权限的鉴别，服务器通过服务请求消息携带的通行证和认证信息确定服务请求消息的发送者和服务授权。当然，如果要求保密客户和服务器之间传输的服务请求和响应消息，可以用客户和服务器约定的会话密钥加密客户和服务器之间传输的服务请求和响应消息。Kerberos 主要功能在于认证请求服务器提供服务的客户的身份并鉴别他的服务权限，所以需要事先建立标识客户的客户名、口令和对应服务权限之间的绑定关系，这种绑定关系通过注册过程建立，并存储在注册信息库中。

TLS 的主要功能是认证访问的服务器，并对客户和服务器之间传输的数据进行加密

和完整性检测，因此，在开始和服务器交换数据前，必须先认证建立会话的服务器的身份，这种认证过程通常通过认证中心签发的证明服务器域名和公钥之间绑定关系的证书和确认服务器拥有证书中给出的公钥所对应的私钥得以实现。因此，在完成服务器身份认证后，客户和服务器之间必须约定加密算法、MAC 算法、加密密钥和 MAC 密钥，确保数据在客户和认证服务器之间的安全传输。当然，TLS 也可实现对客户身份和服务权限的认证和鉴别，这当然需要事先在服务器中建立标识客户的客户名和对应服务权限之间的绑定关系。

除了特定应用需要实现身份认证、数据加密和完整性检测外，许多基于 IP 的其他协议也需要上述功能，如实现 VPN 的隧道协议，就需要对隧道两端的路由器身份进行认证，确保经过隧道传输的数据在传输过程中不被篡改。当然可以分别针对各种基于 IP 的高层协议开发对应的认证协议，但这样做不仅麻烦，而且还需修改这些协议的实现过程。网络分层结构的好处是只要不改变 IP 和这些基于 IP 的协议之间的接口，增强 IP 的安全功能对这些协议而言是透明的，IP 安全协议（IP Security，IPSec）就是一系列用于增强 IP 安全功能的协议。

实现双方身份认证、数据加密和完整性检测涉及认证机制、密钥分配机制、加密和 MAC 机制，认证机制、密钥分配机制用于建立发送者和接收者之间的关联，这种关联通过双方约定的加密和 MAC 算法、加密和 MAC 密钥体现，接收者根据作用于数据的加密算法和加密密钥、MAC 算法和 MAC 密钥确定和其关联的发送者。

3.5.1　安全关联

1．安全关联结构和相关参数

为了确认每一个 IP 分组的发送者，必须建立发送者和接收者之间的关联，这种以认证发送者、进行数据加密和完整性检测为目的的关联称为安全关联（Security Association，SA），安全关联是单向的，用于确定发送者至接收者传输方向的数据所使用的加密算法和加密密钥、MAC 算法和 MAC 密钥。

如果某对发送者和接收者需要安全传输数据，必须先建立发送者至接收者的安全关联，如图 3.54 所示，安全关联用安全参数索引（Security Parameters Index，SPI）、目的 IP 地址和安全协议标识符唯一标识，具有相同接收者的安全关联（目的 IP 地址相同的安全关联）需要分配不同的 SPI，安全协议标识符指定该安全关联使用的安全协议，目前已经定义的安全协议有只对数据进行完整性检测的认证首部（Authentication Header，AH）协议和对数据进行加密和完整性检测的封装安全净荷（Encapsulating Security Payload，ESP）协议。

发送者如果需要安全传输数据给接收者，必须先确定用于安全传输数据的安全关联，如图 3.54 所示，同一对发送者和接收者之间可以建立多个安全关联，因此，发送者不能简单通过数据的接收者确定安全关联，而且，以后的讨论中会指出：数据的目的地和安全关联的目的地可以不同，为此，发送者需要通过定义安全策略数据库（Security Policy Database，SPD）来判别数据传输所使用的安全关联，SPD 的目的是将数据分类，然后将不同类的数据绑定到不同的安全关联，分类数据的依据是数据的源和目的 IP 地址、数据所

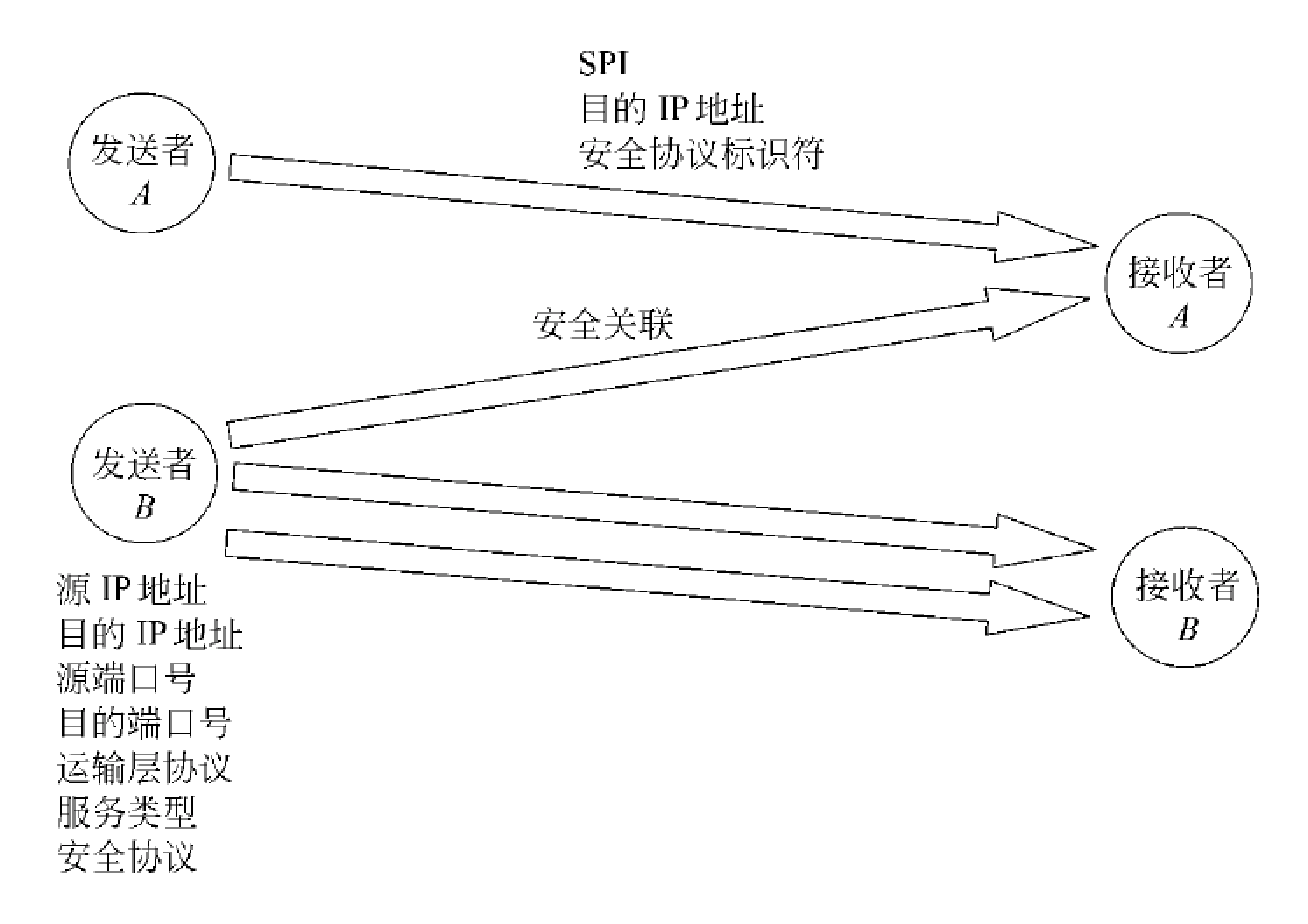


图 3.54 安全关联

使用的运输层协议、运输层源和目的端口号、传输数据使用的安全协议、数据所要求的服务类型等。

为了实现数据发送者至接收者的安全传输，每一个安全关联需要定义下述参数。

- 序号：32位长度，作为AH或ESP首部中序号字段值，用于防止中继攻击(亦称重放攻击)。在安全关联存在期间，不允许出现相同序号的AH或ESP分组。
- 防中继攻击窗口：用于确定接收到的AH或ESP分组是否是中继分组(亦称重放分组)。
- AH信息：MAC算法、MAC密钥、MAC密钥寿命及其他用于AH的参数。
- ESP信息：加密算法和加密密钥、MAC算法和MAC密钥、密钥寿命及其他用于ESP的参数。
- 安全关联寿命：可以是一段用于确定安全关联存在的时间间隔，也可以是安全关联允许发送的字节数，一旦安全关联经过了安全关联寿命定义的时间间隔，或是发送了安全关联寿命允许发送的字节数，将立即终止该安全关联。
- IPSec协议模式：目前定义了两种模式，运输和隧道。
- 路径最大传送单元(Maximum Transfer Unit，MTU)：不用分段可以在安全关联绑定的发送端和接收端之间传输的最大分组长度。

2. 运输和隧道模式

1）运输模式

运输模式用于保证数据端到端安全传输，并对数据源端进行认证，这种模式下，IPSec所保护的数据就是作为IP分组净荷的上层协议数据，如TCP、UDP报文和其他基于IP的上层协议报文。安全关联建立在数据源端和目的端之间，如图3.55所示。

2）隧道模式

隧道模式如图3.56所示，连接源端和目的端的内部网络被一个公共网络分隔，由于

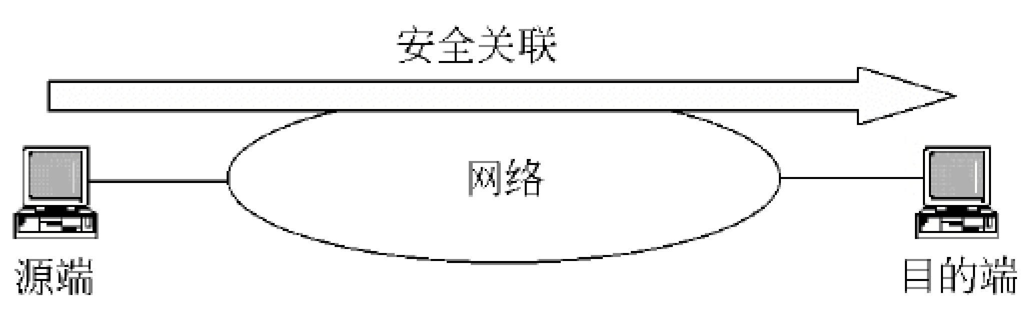


图 3.55　运输模式

内部网络使用本地 IP 地址，而公共网络只能路由以全球 IP 地址为目的 IP 地址的 IP 分组，因此，直接以源端 IP 地址为源 IP 地址、目的端 IP 地址为目的 IP 地址的 IP 分组不能由公共网络正确地从路由器 R_1 路由到路由器 R_2，路由器 R_1 为了将源端至目的端的 IP 分组经过公共网络传输给路由器 R_2，将源端至目的端的 IP 分组作为净荷封装在以路由器 R_1 的全球 IP 地址为源 IP 地址，路由器 R_2 的全球 IP 地址为目的 IP 地址的 IP 分组中，这种将整个 IP 分组作为另一个 IP 分组的净荷的封装方式就是隧道格式，这种情况下，安全关联的两端就是隧道的两端，对于源端至目的端传输方向，安全关联的发送端是路由器 R_1，接收端是路由器 R_2。

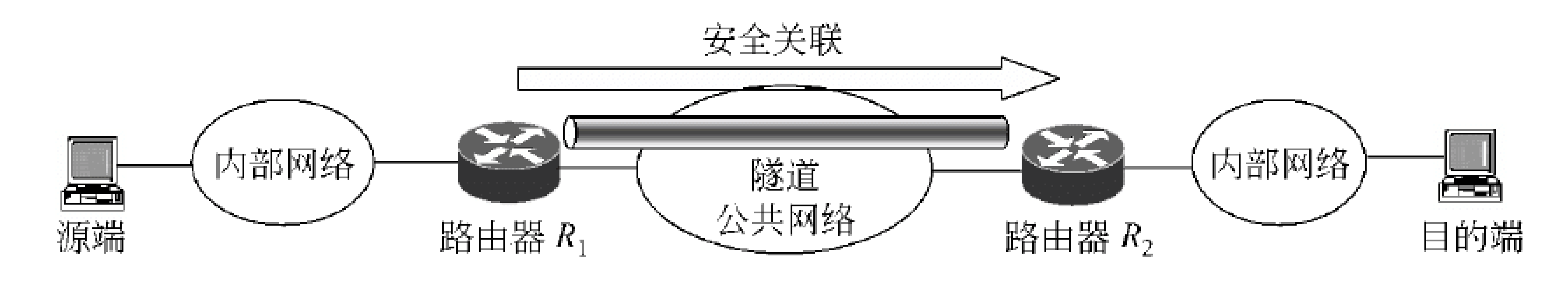


图 3.56　隧道模式

3. 防中继攻击过程

中继攻击（亦称重放攻击）过程如图 3.57 所示，由于 IPSec 对源端至目的端的 IP 分组实现源端认证、数据加密和完整性检测，黑客伪造源端至目的端的 AH 或 ESP 报文是不可能的，即使黑客截获源端至目的端的 AH 或 ESP 报文，也无法篡改，或者解密 AH 或 ESP 报文包含的数据，但黑客可以重复转发截获的 AH 或 ESP 报文，或是延迟一段时间后，再转发截获的 AH 或 ESP 报文，目的端必须能够区分出重复的 AH 或 ESP 报文和因为传输延迟超长而失效的 AH 或 ESP 报文，防中继攻击机制就是解决上述问题的机制。

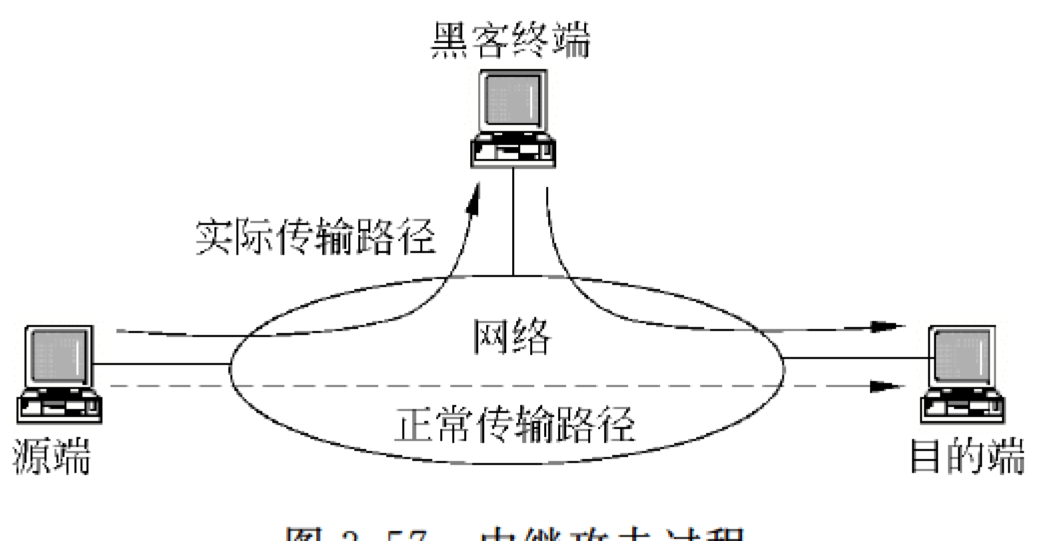


图 3.57　中继攻击过程

源端至目的端的安全关联新建立时，序号初始值为 0，源端发送 AH 或 ESP 报文时，先将序号增 1，然后将增 1 后的序号作为 AH 或 ESP 报文的序号字段值，在安全关联寿命内，不允许出现相同的序号，因此，目的端只要接收到序号重复的 AH 或 ESP 报文，将丢

弃重复接收到的 AH 或 ESP 报文。由于 AH 或 ESP 报文经过 IP 网络传输时不是按序到达目的端，因此，序号小的 AH 或 ESP 报文后于序号大的 AH 或 ESP 报文到达目的端是正常的，但 AH 或 ESP 报文经过 IP 网络传输的延迟抖动有一个范围，如果某个 AH 或 ESP 报文的传输延迟和其他 AH 或 ESP 报文传输延迟的差值超出这个范围，可以认为该 AH 或 ESP 报文被黑客延迟了一段时间。防中继攻击窗口就用于定义正常的延迟抖动范围。假定防中继攻击窗口值为 W，目的端正确接收到的 AH 或 ESP 报文中最大序号值为 N，则序号值为 $N-W+1\sim N$ 的 AH 或 ESP 报文属于虽然传输延迟大于序号为 N 的 AH 或 ESP 报文，但仍在正常的延迟抖动范围内，目的端正常接收这些 AH 或 ESP 报文。

W

序号 N−W+1　　序号 N

未接收该序号对应的报文　　该序号对应的报文已正确接收

图 3.58　防中继攻击机制

对于图 3.58 所示的防中继攻击窗口，目的端每接收到一个 AH 或 ESP 报文，执行如下操作：

- 如果报文序号小于 $N-W+1$，或者该序号对应的报文已经正确接收，丢弃该报文。
- 如果报文序号在窗口范围内，且未接收过该序号对应的报文，接收该报文并将该序号对应的标志改为已正确接收该序号对应的报文。
- 如果报文序号大于 N，假定为 $L(L>N)$，将窗口改为 $L-W+1\sim L$，并将序号 L 对应的标志改为已正确接收该序号对应的报文。

3.5.2　AH

IP 分组封装成 AH 报文的过程如图 3.59 所示，运输模式下，在 IP 首部和净荷之间插入认证首部 AH，隧道模式下，整个 IP 分组作为隧道格式的净荷，在外层 IP 首部和净荷之间插入认证首部 AH，认证首部格式如图 3.60 所示，各个字段的含义如下。

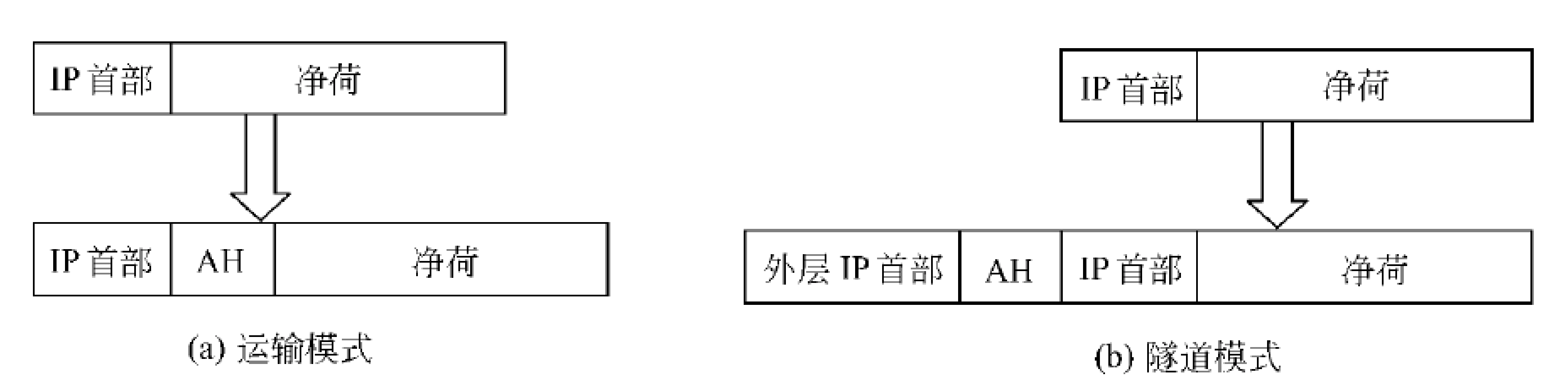


图 3.59　AH 报文格式

8位	8位	16位
下一个首部	认证首部长度	保留
安全参数索引 (SPI)		
序号		
认证数据		

图 3.60　认证首部(AH)格式

- 下一个首部：指出净荷的协议类型，封装成 AH 报文后，IP 首部中的协议字段值为 51，表明是 AH 报文，IP 首部中用于指明净荷协议类型的协议字段值作为 AH 中的下一个首部。
- 认证首部长度：以 32 位为单位给出 AH 的总长，实际的认证首部长度是 AH 总长－2，一般情况下，认证数据为 96 位，3 个 32 位字，因此，图 3.54 所示的 AH 的总长为 6 个 32 位字，使得认证首部长度字段的值为 4。
- 安全参数索引(SPI)：接收端将其和 AH 报文的目的 IP 地址和 IP 首部中 IPSec 协议类型一起用于确定 AH 报文所属的安全关联。
- 序号：用于防中继攻击。
- 认证数据：消息认证码(MAC)，用于认证源端身份和进行数据完整性检测。

认证数据的计算可以采用如下两种 MAC 算法。

(1) HMAC-MD5-96；

(2) HMAC-SHA-1-96。

这两种算法表明采用 3.2.4 节给出的 HMAC—基于密钥的报文摘要计算过程时，报文摘要算法可以选择 MD5(HMAC-MD5-96)或 SHA-1(HMAC-SHA-1-96)，从计算得到的加密报文摘要中截取 96 位作为认证数据。建立安全关联时，源端和目的端必须约定所采用的 HMAC 算法和 MAC 密钥。

计算认证数据时覆盖 AH 报文下述字段。

- IP 首部(隧道模式下是外层 IP 首部)中传输过程中无须改变的字段值，如源和目的 IP 地址等。
- AH 中除了认证数据的其他字段值，如 SPI、序号等。
- AH 报文中的净荷，如果是隧道模式，净荷是包括内层 IP 首部的整个 IP 分组。

传输过程中一旦篡改某个计算认证数据时覆盖的字段值，目的端重新计算后得出的认证数据和 AH 中包含的认证数据不符，目的端因此确定该 AH 报文认证失败，因此，目的端认证成功的前提是：

① 源端和目的端采用相同的 HMAC 算法和 MAC 密钥；

② 计算认证数据所覆盖的字段值在传输过程中未被篡改。

3.5.3　ESP

IP 分组封装成 ESP 报文的过程如图 3.61 所示，运输模式下，IP 首部和净荷之间插入 ESP 首部，如图 3.62 所示，ESP 首部包含安全参数索引(SPI)和序号，它们的作用和 AH 相同。净荷字段后面是 ESP 尾部，它们包括填充数据、8 位填充长度字段和 8 位下一个首部，填充长度字段值以字节为单位给出填充数据长度，下一个首部给出净荷的协议类型。净荷后面添加填充数据的目的一是为了对净荷进行加密运算时，保证净荷＋ESP 尾部是数据组长度的整数倍，如 DES 加密算法的数据组长度为 64 位；二是净荷＋ESP 尾部必须是 32 位的整数倍；三是隐藏实际净荷长度有利于数据传输的安全性。隧道模式下，净荷是包括内层 IP 首部在内的整个 IP 分组。

ESP 加密运算覆盖的字段是净荷＋ESP 尾部，可以在以下多种加密算法中任选一种

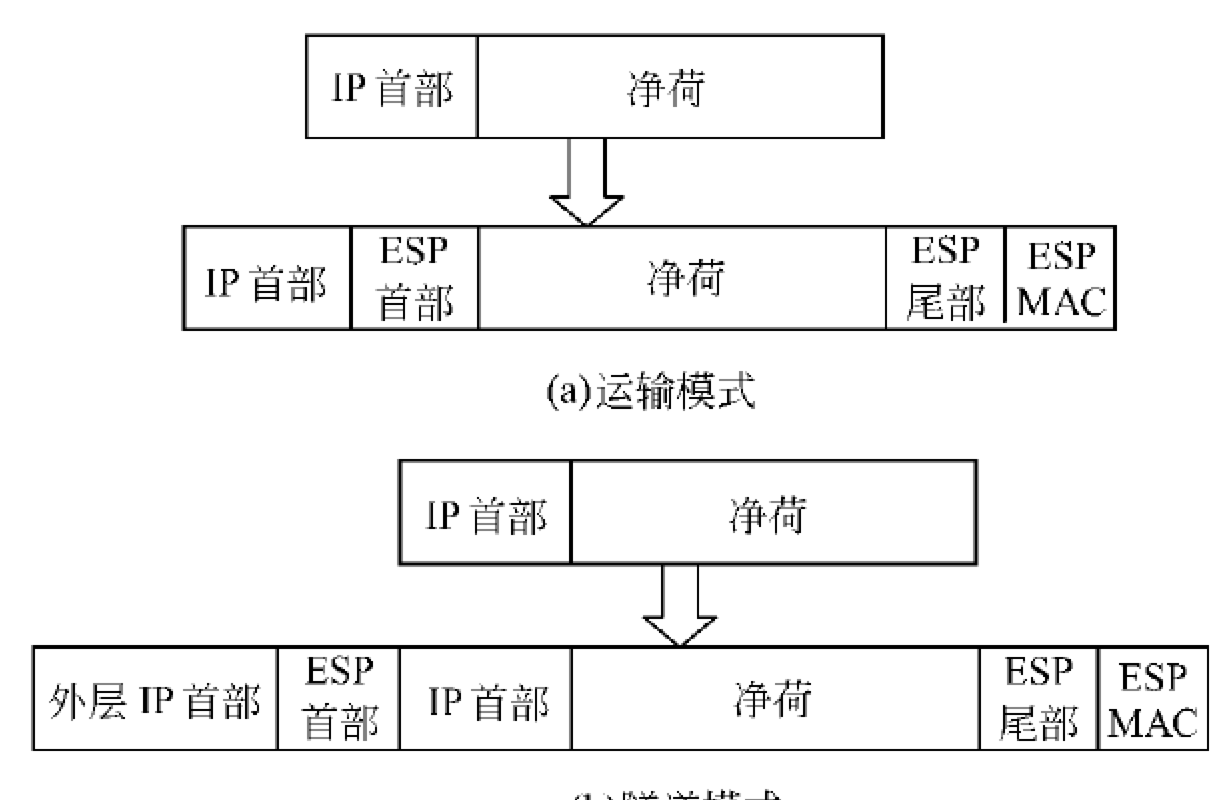


图 3.61 ESP 报文格式

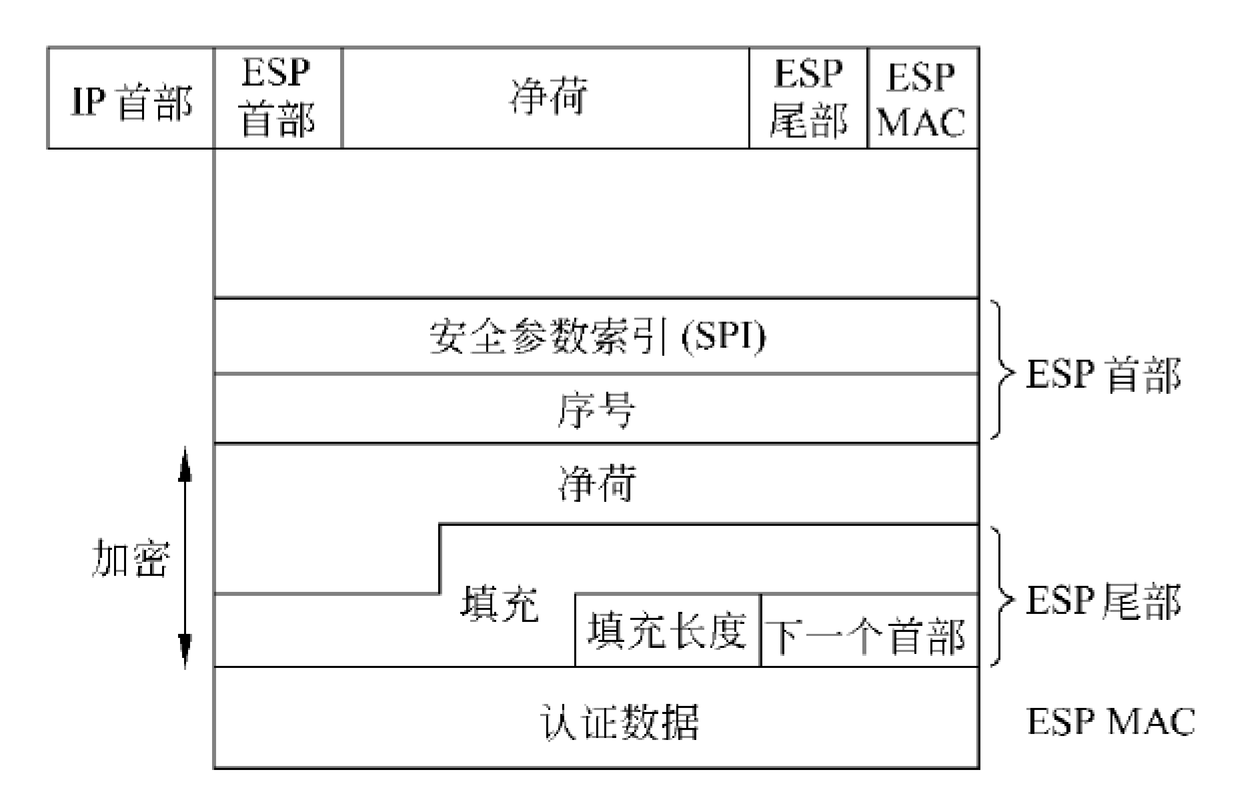


图 3.62 ESP 首部、尾部和 MAC 格式

加密算法,但常用的加密算法是三重 DES。

- 三重 DES;
- RC5;
- IDEA;
- 三重 IDEA。

采用和 AH 相同的 MAC 算法计算认证数据,但计算认证数据时覆盖的字段只包括 ESP 首部+净荷+ESP 尾部。并不包括外层 IP 首部中的不变字段,这一点和 AH 不同。隧道模式下,净荷是包括内层 IP 首部在内的整个 IP 分组。

3.5.4 ISAKMP

发送者和接收者之间建立安全关联时必须完成:

- 双方身份认证;
- 约定 IPSec 协议(AH 或 ESP)和 SPI;
- 如果采用 ESP IPSec 协议,约定加密算法和加密密钥;

• 约定认证算法和 MAC 密钥。

Internet 安全关联和密钥管理协议（Internet Security Association and Key Management Protocol，ISAKMP）就是一种用于建立安全关联并实现上述功能的协议。但 ISAKMP 只是一种承载协议，并不提供实现上述功能的机制，只是提供用于传输特定认证机制和密钥交换机制所需要的信息的方法和格式。

前面各节已经讨论了多种用户身份认证和密钥交换机制，如 Kerberos 中基于对称密钥算法的认证和密钥交换机制，TLS 中基于公开密钥算法的认证机制和密钥交换机制和 Diffie-Hellman 密钥交换机制，这些机制和算法均可作为 ISAKMP 的认证机制和密钥交换机制，下面通过一个实例介绍一下 ISAKMP 建立安全关联过程。

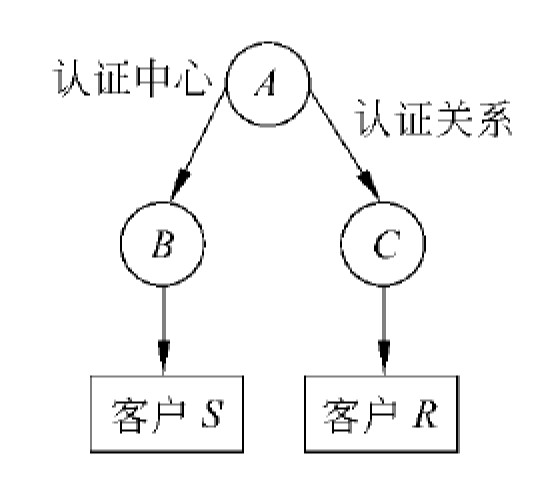


图 3.63　证书链

假定发送者和接收者的用户名分别是 ID_S 和 ID_R，认证中心用于证明用户名和公钥之间绑定关系的证书链如图 3.63 所示，双方均拥有认证中心 *A* 的公钥 PKA，因而能够确认认证中心 *A* 签发的证书。发送者和接收者均通过配置建立允许建立安全关联的用户名列表，发送者希望和接收者建立的安全关联需要约定下述安全参数。

• IPSec 协议：ESP。
• 加密算法：三重 DES。
• 认证算法：HMAC-MD5-96。
• 安全参数索引：SPI。
• 加密密钥和 MAC 密钥动态生成。

双方开始建立安全关联前，必须先交换证书链，当然，无须每一次建立安全关联都交换证书链。建立安全关联的过程就是认证对方身份和约定安全参数的过程，如图 3.64 所示，发送者发送给接收者的第一个 ISAKMP 消息中给出选定的 IPSec 协议 ESP 及采用的加密算法三重 DES 和认证算法 HMAC-MD5-96，SPI，用户名 ID_S、Diffie-Hellman 公钥 YS 和随机数 NS，为了证明发送者的身份，并对传输的数据进行完整性检测，发送者用公钥 PKS 对应的私钥 SKS 对上述数据的报文摘要进行 RSA 解密运算。接收者用证书 *B* <<客户 *S*>>中给出的公钥 PKS 对密文进行 RSA 加密运算，获得发送端计算的报文摘要，并重新对明文给出的数据进行报文摘要运算，如果运算结果和加密运算得到的数据相等，意味着发送者的用户名确实是 ID_S，且该 ISAKMP 消息在传输过程中未被篡改。

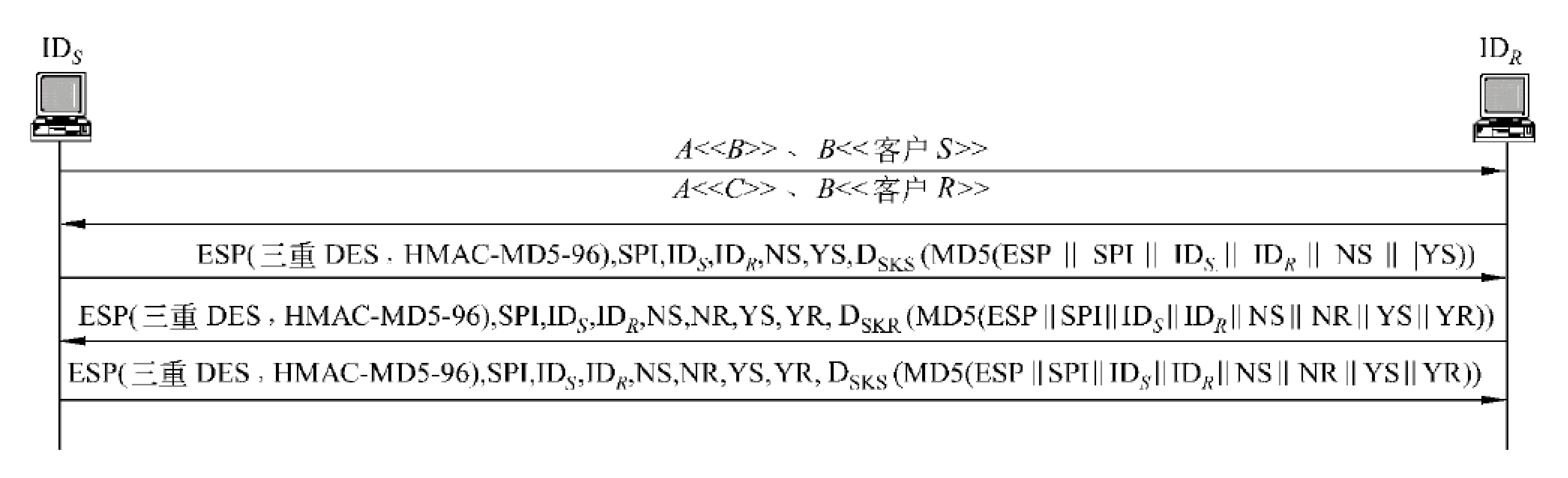


图 3.64　ISAKMP 建立安全关联过程

由于双方采用 Diffie-Hellman 密钥交换机制，给出的公钥 YS 用于计算双方约定的加密密钥和 MAC 密钥，随机数 NS 是为了防止中继攻击。

接收者在确认发送者身份，并同意发送者选择的安全参数后，向发送者回送一个响应消息，响应消息中不仅给出发送者选择的安全参数，还给出接收者选择的 Diffie-Hellman 公钥 YR 和随机数 NR，为了让发送者证实接收者的身份，同时也为了进行数据的完整性检测，接收者同样用公钥 PKR 对应的私钥 SKR 对上述数据的报文摘要进行 RSA 解密运算。

发送者完成对接收者的身份认证后，确定双方已经约定安全参数，将双方约定的安全参数再次发送给接收者，表明发送者已经确定该安全关联所使用的安全参数，接收者将发送者最后确定的安全参数和自己保留的安全参数比较，比较无误后，表明安全关联成功建立，否则，需要向发送者发送安全参数有错的通知消息。

发送者和接收者根据对方发送的公钥，计算会话密钥 K 的过程如下：

$$K=\mathrm{YS}^{\mathrm{XR}} \bmod q=\mathrm{YR}^{\mathrm{XS}}\ \mathrm{mode}\ q$$

XS 和 XR 是发送者和接收者选择的私钥，q 为一个大素数，三重 DES 所需要的 3 个加密密钥和计算 MAC 所需要的 MAC 密钥，由 K 推导出。

ISAKMP 为了适应多种认证机制和密钥交换机制，只定义了传输对应机制所需要数据的净荷格式，具体的数据格式由各种机制自行定义。

如果需要对建立安全关联时交换的 ISAKMP 消息进行加密处理，在开始安全关联建立过程前，需要先建立发送端和接收端之间的安全传输通道，建立安全传输通道的目的是在发送端和接收端之间约定加密 ISAKMP 消息使用的加密算法和加密密钥。建立发送端和接收端之间的安全传输通道的过程和建立安全关联的过程非常相似，这里不再赘述，后面章节有关 IPSec 的应用实例中将有所讨论。

习　题

3.1　RSA 私钥和对称密钥加密算法中的密钥有什么不同？

3.2　DES 和 AES 对称密钥加密算法如此复杂的原因是什么？

3.3　一些检错码，如检验和、循环冗余检验码是否具有消息认证码(MAC)的特性？它们无法成为实际使用的 MAC 的原因是什么？MD5 和 SHA-1 能否成为计算检错码的算法？实际应用中不将它们作为计算检错码算法的原因是什么？

3.4　什么是数字签名？它和发送端身份认证有什么区别？

3.5　用户 A 的 RSA 公钥和私钥对为 PKA、SKA，用户 B 的 RSA 公钥和私钥对为 PKB 和 SKB，如果用户 B 需要确定数据发送者是用户 A，而用户 A 只希望用户 B 能读取数据，用户 A 如何封装数据？如果用户 A 将发送大量数据给用户 B，如何解决发送端身份认证和数据加密问题？

3.6　根据下值，给出 RSA 加密、解密运算过程：

(1) $p=3, q=11, e=7, M=5$；

(2) $p=5, q=11, e=3, M=9$；

(3) $p=7, q=11, e=17, M=8$。

3.7　根据 Diffie-Hellman 计算密钥机制，假定素数 $q=11$，原根 $\alpha=2$，完成下列计算：

(1) 用户 A 公钥 $Y_A=9$，计算私钥 X_A；

(2) 用户 B 公钥 $Y_B=3$，计算共享密钥 K。

3.8　列出发送端身份认证机制并比较它们的特点。

3.9　列出接收端身份认证机制并比较它们的特点。

3.10　802.1X 如何确认数据发送端？

3.11　流密码体制和分组密码体制有什么区别？什么条件下流密码体制是安全的？

3.12　置换和替代运算有什么区别，给出置换和替代运算实例。

3.13　为什么三重 DES 加密运算过程的中间运算步骤是 DES 解密运算？

3.14　给出所有实现通信双方安全分发密钥的机制。

3.15　解释 TLS 采用如此复杂的加密密钥、MAC 密钥计算过程的原因。

3.16　用户 A 为了确认用户 B 拥有和自己相同的密钥 K，生成一个和密钥 K 相同长度的随机数 C，对随机数 C 和 K 进行异或运算，并将运算结果发送给用户 B，用户 B 用自己的密钥异或用户 A 发送的数据，并将计算结果返还给用户 A，如果用户 B 返还给用户 A 的结果就是随机数 C，表明用户 B 拥有和用户 A 相同的密钥，这种确认双方密钥的机制有什么缺点？

3.17　如果用户 A 需要用对称密钥算法加密发送给用户 B 的数据，但需要根据用户 B 用明文方式发送的信息计算出对称密钥，有什么好的方法可以避免黑客通过截获用户 B 用明文方式发送的信息得出用户 A 用于加密数据的对称密钥。

3.18　试给出 IPSec 应用实例。

3.19　发送端如何确定本次数据传输所关联的安全关联，接收端如何确定接收到的数据所关联的安全关联。

3.20　隧道模式和运输模式有什么区别？

3.21　什么是中继攻击？IPSec 如何防中继攻击？

3.22　TLS 是否具有防中继攻击机制？如何解决经过 TLS 传输的数据的有效性检测？

3.23　AH 计算 MAC 时，外层 IP 首部中哪些字段是不包含在内的？为什么？

3.24　隧道模式构建外层 IPv4 首部时，如何确定首部各个字段值？哪些字段值的确定和内层 IPv4 首部有关？

3.25　有哪些机制可用于建立安全关联？建立安全关联需要确定哪些参数？

3.26　如果图 3.65 中源端发送给目的端的数据经过公共网络传输时要求保密性和完整性，给出安全关联参数，并给出数据经过公共网络传输时的封装格式。

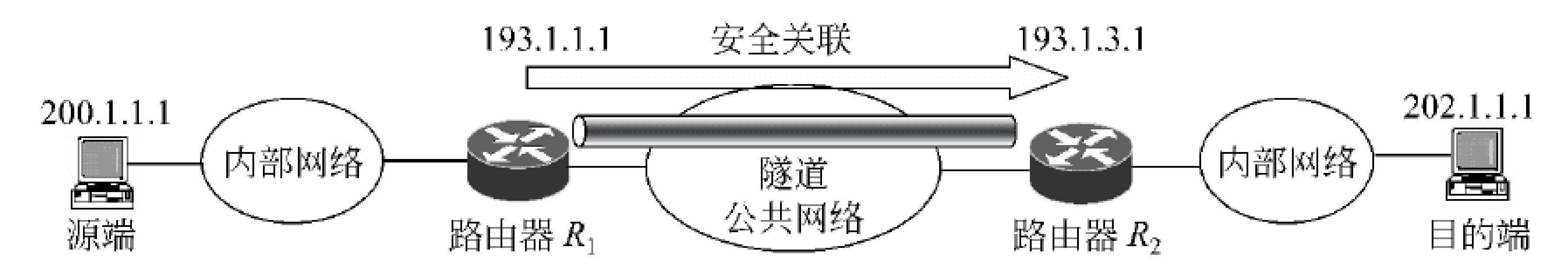


图 3.65　题 3.26 图

3.27 图 3.66 是一个校园网逻辑结构图，如果要求对接入校园网的学生终端进行身份认证，如何配置该网络，并给出控制某个学生终端接入网络的全过程。

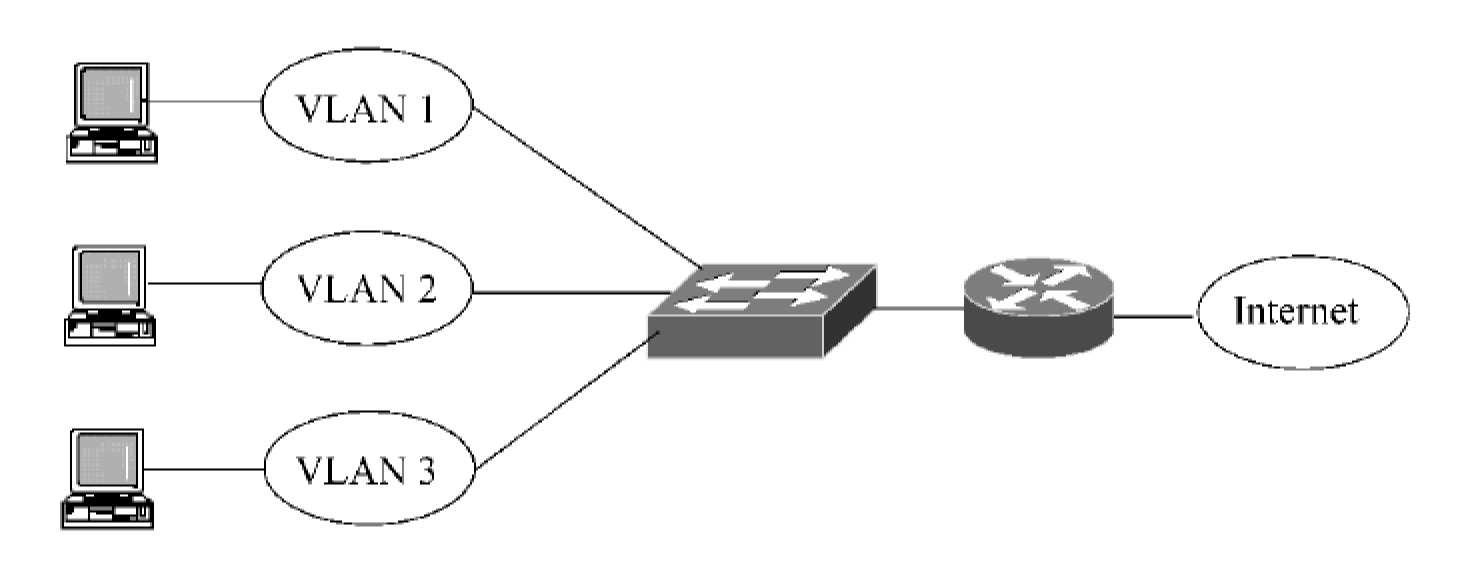


图 3.66 题 3.27 图

第 4 章 安全网络技术

CHAPTER

人们发明网络的原旨是实现相互通信，共享信息资源，因此，网络的结构不仅带有开放性，而且一切都是为方便通信和资源访问而设计的，但这种特性目前却成了网络安全的最大隐患，因此，解决网络安全问题的第一步就是提高网络对接入终端的认证能力，对用户信息流模式的控制能力，及对用户带宽的管制能力等。

4.1 以太网安全技术

从图 4.1 所示的 Internet 组成可以看出，直接连接用户终端的网络是接入网和校园网（或局域网），而以太网是目前最常见的用作接入网和校园网的传输网络，因此，大多数用户终端通过以太网接入 Internet，以太网的安全性直接影响着整个网络的安全性。

4.1.1 以太网接入控制

1. 访问控制列表

访问控制列表是以太网控制终端接入的一种机制，以太网交换机的每一个端口可以单独配置访问控制列表，访问控制列表中列出允许接入的终端的 MAC 地址，如图 4.2 中为以太网交换机端口 F0/1 定义的访问控制列表表明该端口只允许接入 MAC 地址为 00-46-78-11-22-33 的终端，因此，从该端口接收到的 MAC 帧中，只有源 MAC 地址等于 00-46-78-11-22-33 的 MAC 帧才能继续转发，其他 MAC 帧都被该端口丢弃。当终端 *A* 接入端口 F0/1 时，由于终端 *A* 发送的 MAC 帧的源 MAC 地址等于 00-46-78-11-22-33，因而能够被以太网交换机转发，当其他终端，如终端 *B*，接入端口 F0/1 时，由于其发送的 MAC 帧的源 MAC 地址不等于 00-46-78-11-22-33，以太网交换机将丢弃这些 MAC 帧。每一个端口配置的访问控制列表中可以有多个 MAC 地址，因而允许多个其 MAC 地址和访问控制列表中的某个 MAC 地址相同的终端接入该端口，当然，对于图 4.2 所示的连接方式，任何时候，每个以太网交换机端口只能接入单个终端。

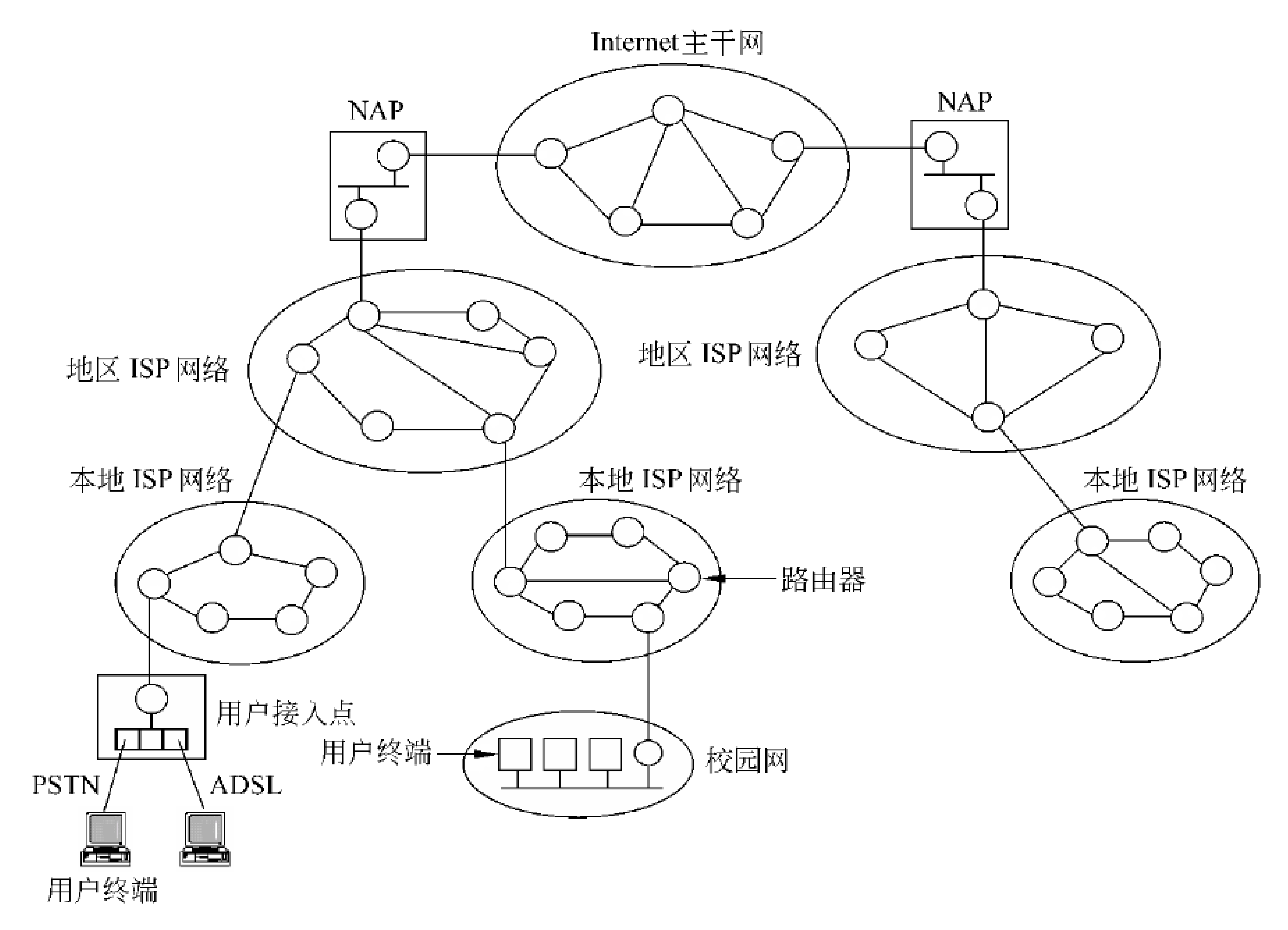


图 4.1 Internet 组成

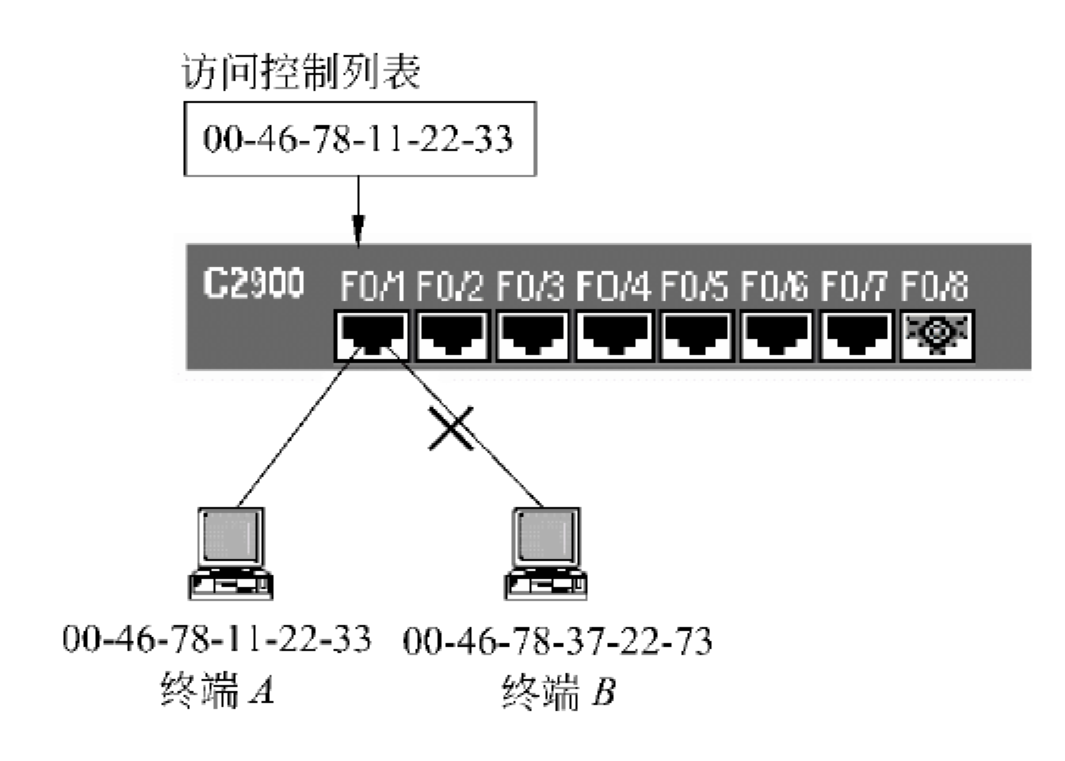


图 4.2 访问控制列表控制终端接入过程

2. 安全端口

手工配置以太网交换机每一个端口的访问控制列表是一件十分麻烦的事情，安全端口技术提供了一种自动生成每一个端口的访问控制列表的机制。安全端口技术可以为每一个端口设置自动学习到的 MAC 地址数 N，这样，从进入该端口的 MAC 帧的源 MAC 地址中学习到的最先 N 个 MAC 地址，自动成为访问控制列表中的 MAC 地址，以后，也只有源 MAC 地址属于这 N 个 MAC 地址的 MAC 帧才能继续转发，其他 MAC 帧都被该端口丢弃。如果将 N 设置为 1，首先将终端 A 接入端口 F0/1，端口 F0/1 生成的访问控制列表如图 4.2 所示，以后只有终端 A 发送的 MAC 帧才能继续转发，其他终端接入端口 F0/1 后发送的 MAC 帧都被该端口丢弃。

3. 802.1X 接入控制过程

无论是手工配置访问控制列表方式还是通过安全端口技术自动生成访问控制列表方式都不能动态改变访问控制列表中的 MAC 地址，由于终端的 MAC 地址是可以设定的，一旦某个攻击者获取了访问控制列表中的 MAC 地址，就可以通过将自己终端的 MAC 地址设置为访问控制列表中的某个 MAC 地址实现非法接入，因此，这种通过 MAC 地址来标识允许接入的终端方式在目前允许终端任意设定 MAC 地址的情况下，是不够安全的。安全的接入控制是用用户名和口令来标识合法用户终端，每当有新的终端接入某个端口时，端口能够要求接入终端提供用户名和口令，只有能够提供有效用户名和口令的终端的 MAC 地址，才能进入访问控制列表，一旦该终端离开该端口，或设定时间内该终端一直没有通过该端口发送 MAC 帧，该终端的 MAC 地址将自动从访问控制列表中删除，这就防止了其他终端通过伪造该终端的 MAC 地址非法接入以太网的情况发生。

实现 802.1X 接入控制过程的网络结构如图 4.3 所示，以太网交换机为认证者，需要配置认证服务器的 IP 地址和共享密钥，接入控制可以基于端口或基于 MAC 地址，在基于端口方式下，在完成认证后，端口从非认证状态(也称非授权状态)转变为认证状态(也称授权状态)，允许转发从该端口接收到的所有 MAC 帧。如果将交换机 *A* 端口 F0/7 设置成认证端口，只要终端 *A* 通过了认证，终端 *B* 发送的 MAC 帧也能被交换机 *A* 正常转发。基于端口的 802.1X 接入控制过程一般用于直接连接终端的接入交换机，如交换机 *B*，交换机加电后，或检测到有终端接入某个端口，该端口的状态设置成非认证状态，不允许转发接入终端发送的数据帧，只有通过图 4.4 所示的认证过程，该端口才能从非认证状态转变为认证状态，允许正常转发接入终端发送的数据帧。基于 MAC 地址的接入控制方式是访问控制列表和基于端口的接入控制方式的结合，一旦某个端口完成认证过程，发起该次认证过程的终端的 MAC 地址被添加到访问控制列表中，以后，只有源 MAC 地址和该端口的访问控制列表中的某个 MAC 地址相同的 MAC 帧才能被该端口接收，并被以太网交换机正常转发。在基于 MAC 地址的接入控制方式下，即使终端 *A* 完成了认证过程，交换机 *A* 端口 F0/7 也只能转发终端 *A* 发送的 MAC 帧，终端 *B* 只有发起并完成认证过程后，才能通过交换机 *A* 端口 F0/7 正常转发 MAC 帧。

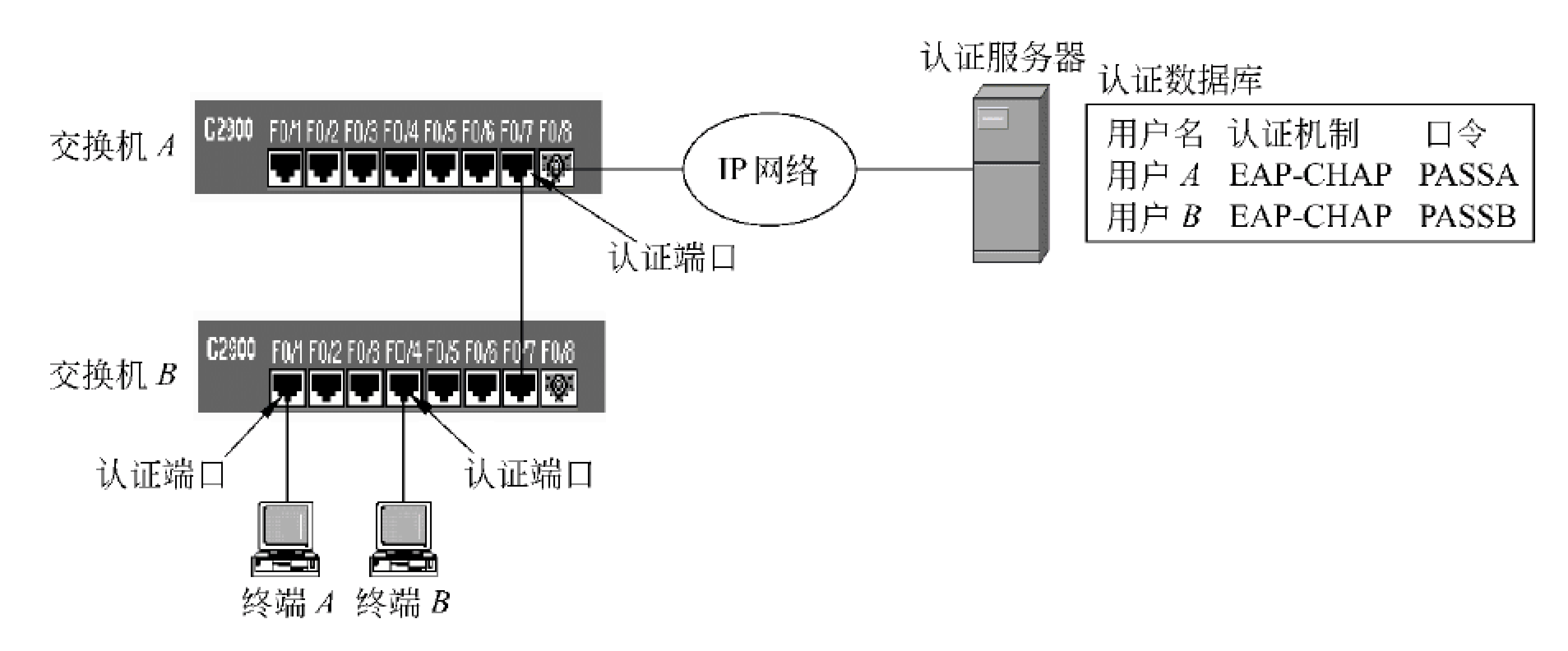


图 4.3　网络结构图

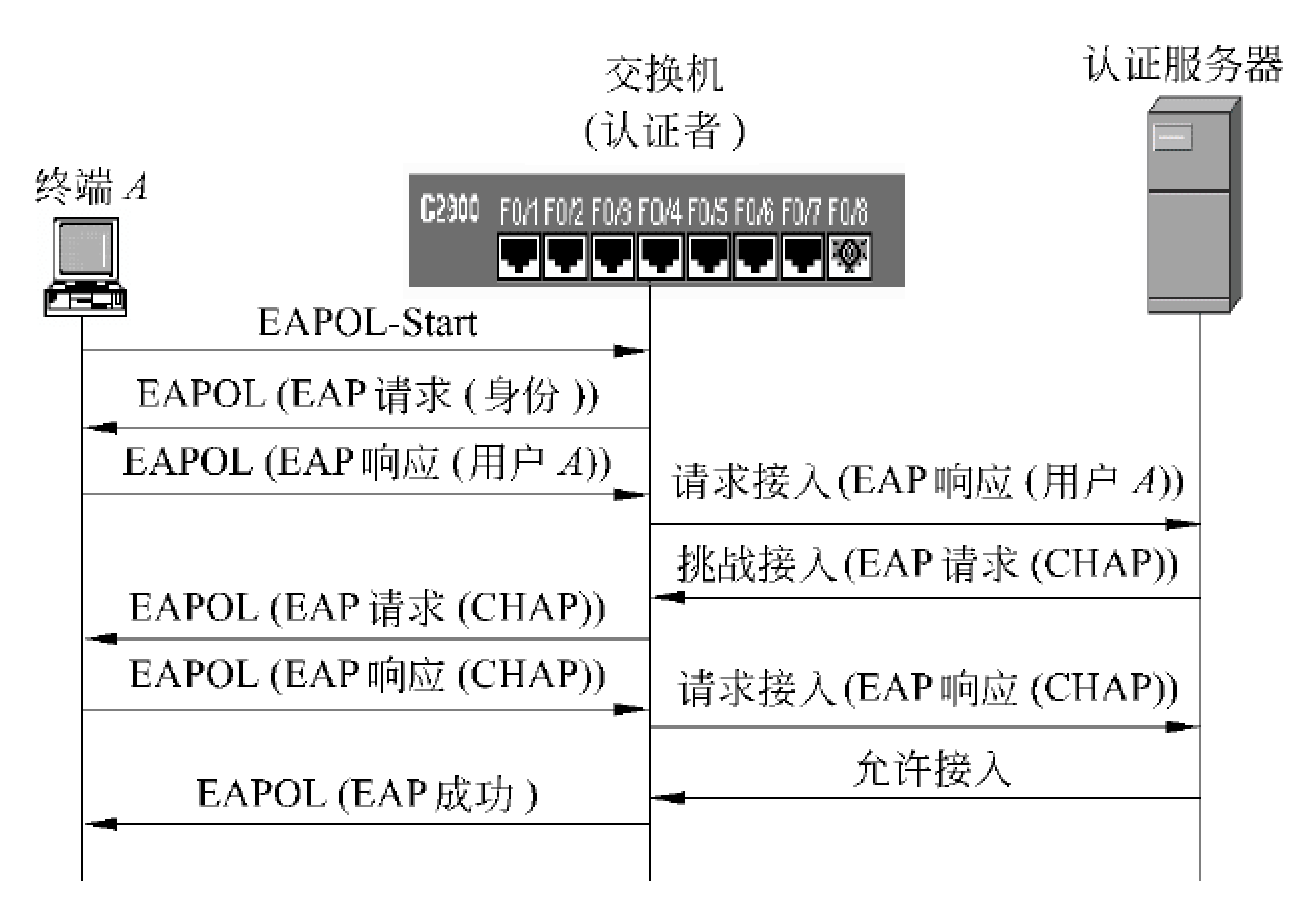


图 4.4 802.1X 接入控制过程

基于 MAC 地址接入控制方式下从端口访问控制列表中删除某个终端的 MAC 地址的情况如下：

- 终端通过 EAPOL-Logoff 退出认证状态。
- 端口在规定时间内一直没有接收到以该 MAC 地址为源 MAC 地址的 MAC 帧。

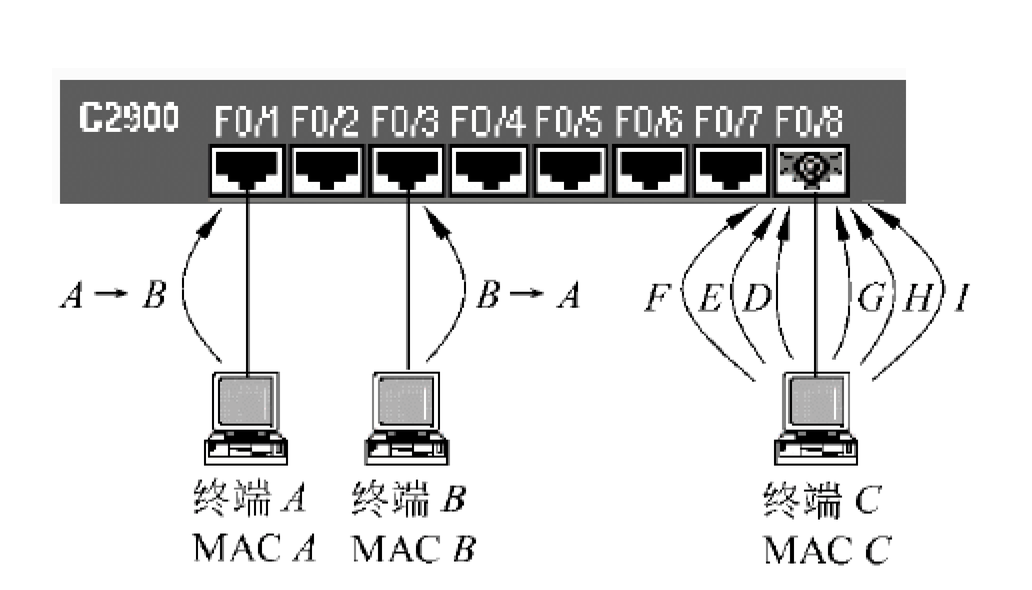
基于端口接入控制方式下将端口状态从认证状态转变为非认证状态的情况如下：

- 终端通过 EAPOL-Logoff 退出认证状态。
- 端口在规定时间内一直没有接收到 MAC 帧。
- 端口检测不到物理连接存在。

4.1.2 以太网其他安全功能

1. 防站表溢出攻击功能

以太网交换机根据站表转发 MAC 帧，站表中的各项通过地址学习获得，如果交换机在站表中找不到和某个 MAC 帧的目的 MAC 地址匹配的项，交换机将广播该 MAC 帧。站表中各项都有寿命，如果在寿命内一直接收不到源地址和该项的 MAC 地址匹配的 MAC 帧，表明寿命溢出，将从站表中删除该项。一旦站表被填满，交换机将停止地址学习，直到站表中某个项因为寿命溢出而被删除。交换机的站表容量必须充分考虑交换机可能学习到的地址数，因此，接入交换机的站表容量较小，核心交换机的站表容量相对较大，正常使用下，不会发生站表被填满的情况。如果图 4.5 中的终端 C 已经被黑客控制，它可以发出大量 MAC 帧，而且，每一个 MAC 帧的源地址都是随机生成的假地址，这些不同的假地址被交换机学习后，成为站表中不同的项，并因此填满站表，当正常终端，如图 4.5中的终端 A，发送 MAC 帧时，由于交换机的站表已经填满，无法学习到该终端的 MAC 地址，因此，当其他终端向该终端发送 MAC 帧时，如图 4.5 中终端 B 向终端 A 发送 MAC 帧的情况，因为站表中找不到和 MAC A 匹配的项，交换机将广播该 MAC 帧，这一方面将极大地浪费网络带宽和终端的处理能力，另一方面将使黑客终端，如终端 C，截获其他终端之间正常交换的 MAC 帧，这就是站表溢出攻击。



站表

端口	MAC 地址
8	MAC *D*
8	MAC *E*
8	MAC *F*
8	MAC *G*
8	MAC *H*
8	MAC *I*

图 4.5　站表溢出攻击

防站表溢出攻击机制非常简单，就是增加设定每一个端口允许学习到的最大地址数的功能，这样，当通过某个端口学习到的地址数超过设定的上限时，不再将通过该端口学习到的新地址记录到站表中，避免发生因图 4.5 中终端 *C* 发起的站表溢出攻击而使站表填满的情况。

2. 防 DHCP 欺骗

动态主机配置协议(Dynamic Host Configuration Protocol，DHCP)用于自动配置终端接入网络所需要的信息，如 IP 地址、子网掩码、默认网关地址等，由于终端在完成自动配置前，没有任何有关网络中资源的信息，因此，也不可能对提供自动配置服务的 DHCP 服务器进行认证，自动配置过程成了网络安全的软肋。

图 4.6 给出了实现 DHCP 欺骗攻击的网络结构，图 4.7 给出了 DHCP 欺骗攻击过程。黑客将伪造的 DHCP 服务器接入以太网，如果新接入以太网的终端设置为自动配置方式，终端将广播一个发现报文，发现报文的作用是用于发现网络中的 DHCP 服务器，网络中的所有终端和服务器都接收到发现报文，但只有 DHCP 服务器对发现报文作出响应。如果某个 DHCP 服务器能够为该终端提供配置信息，通过广播应答报文向该终端表明态度，如果网络中有多个 DHCP 服务器能够为该终端提供配置信息，终端往往选择最先发送应答报文的 DHCP 服务器为其提供配置服务，终端在选定为其提供配置服务的 DHCP 服务器后，向其发送请求报文，并在请求报文中给出选定的 DHCP 服务器的标识符，被终端选定的 DHCP 服务器通过确认报文完成对终端的配置。图 4.7 中，如果伪造的 DHCP 服务器先一步向终端发送了应答报文，终端将选择伪造的 DHCP 服务器提供配置服务，伪造的 DHCP 服务器往往将自己的 IP 地址作为默认网关地址提供给终端，终端所有发送给网络的信息，将首先发送给伪造的 DHCP 服务器。

以太网解决 DHCP 欺骗攻击的机制是将以太网交换机端口配置为信任端口和非信任端口，只有从信任端口接收到的 DHCP 响应报文，如应答报文和确认报文，才能继续转发，所有从非信任端口接收到的 DHCP 响应报文一律丢弃。只有直接连接 DHCP 服务器的端口和用于互连交换机的端口才被配置成信任端口，其他端口一律配置为非信任端口。这样，只有从连接信任端口的 DHCP 服务器发送的响应报文才能到达终端，其他伪造的 DHCP 服务器发送的响应报文都被以太网交换机丢弃。

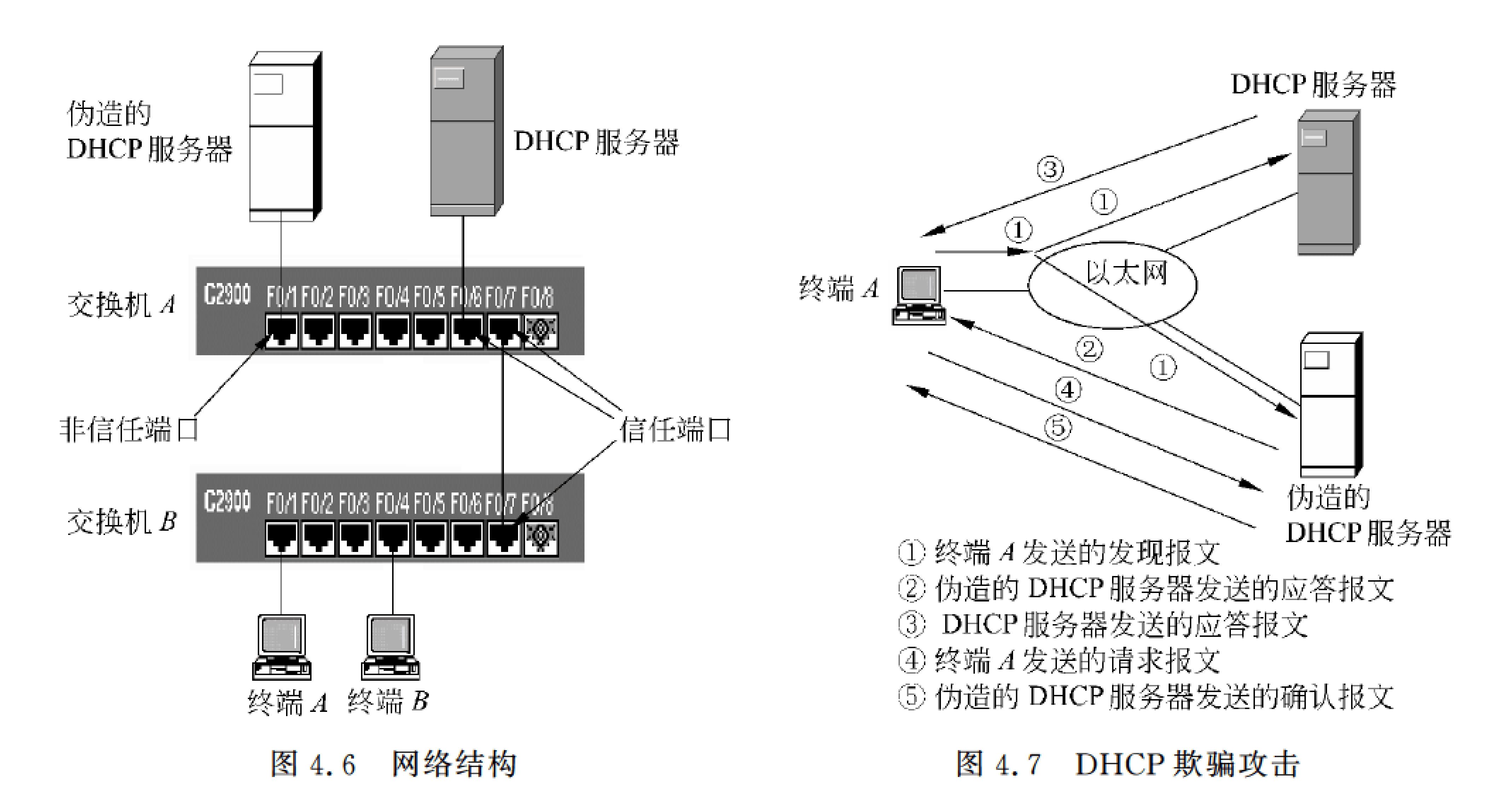


图 4.6　网络结构　　　　图 4.7　DHCP 欺骗攻击

3. 防 ARP 欺骗攻击

图 4.8 是一个普通的以太网结构，图 4.9 给出了终端 *B* 实施 ARP 欺骗攻击的过程，终端 *B* 广播一个将终端 *A* 的 IP 地址 IP *A* 和自己的 MAC 地址 MAC *B* 绑定在一起的 ARP 报文，导致以太网中其他终端将 IP *A* 和 MAC *B* 之间的绑定关系记录在 ARP cache 中，当这些终端需要转发目的 IP 地址为 IP *A* 的 IP 分组时，用 MAC *B* 作为封装该 IP 分组的 MAC 帧的目的 MAC 地址，使得所有原本发送给终端 *A* 的 IP 分组，都被转发给终端 *B*。

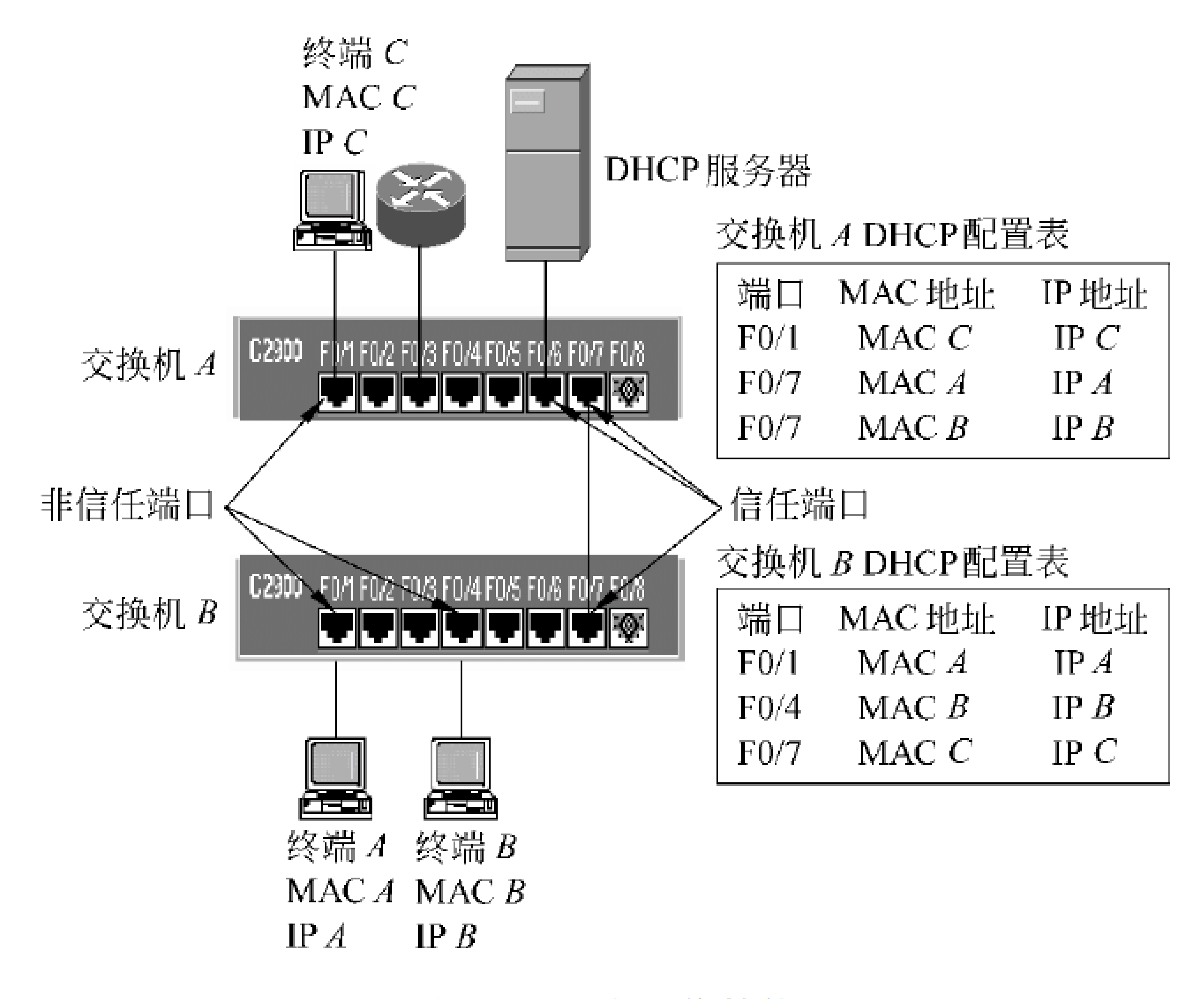


图 4.8　以太网络结构

终端能够实施 ARP 欺骗攻击的原因是网络中任何一个终端无法获得其他终端的配置信息，因而也无法对 ARP 报文中给出的 IP 地址和 MAC 地址之间的绑定关系进行确

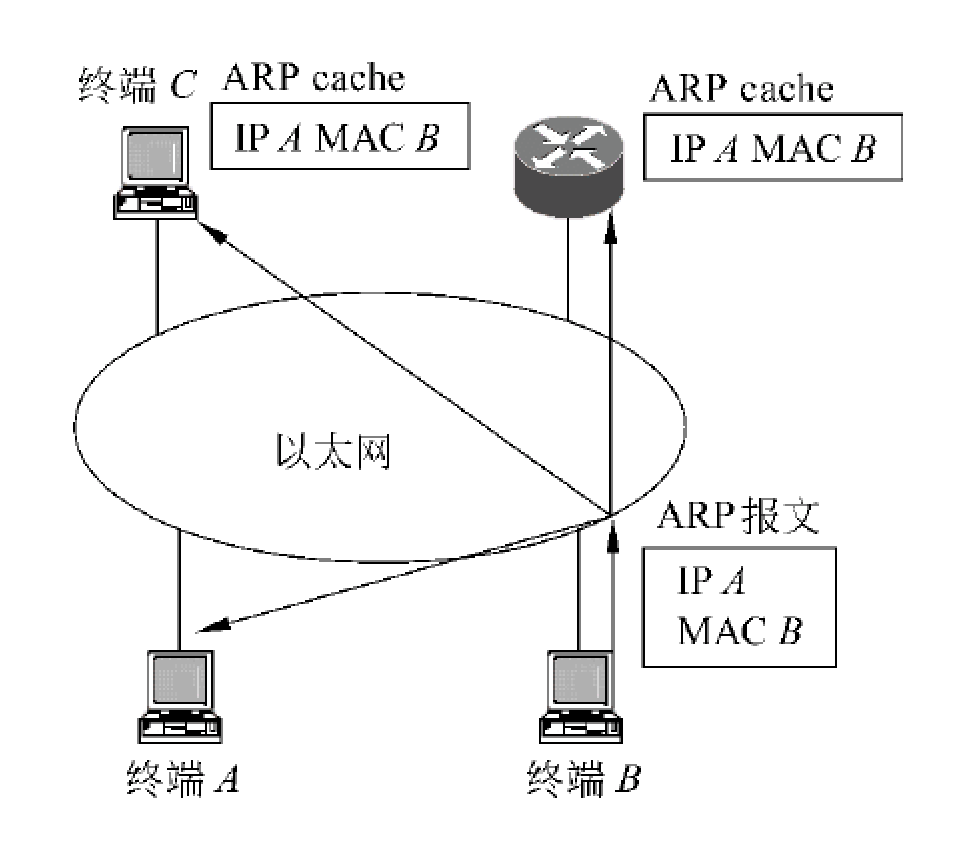


图 4.9　ARP 欺骗攻击过程

认。如果以太网中所有终端都通过 DHCP 自动配置过程配置网络信息，则每一个终端都经历过广播发现报文、接收应答报文、发送请求报文，接收确认报文这样的交互过程，发现和请求报文中将给出终端标识符 MAC 地址，而应答和确认报文中将给出终端标识符和分配给该终端的 IP 地址之间的绑定关系，如果以太网交换机能够侦听 DHCP 报文，并将 DHCP 报文中给出的终端标识符和分配给该终端的 IP 地址之间的绑定关系记录在 DHCP 配置表中，交换机就具有认证 ARP 报文中给出的 MAC 地址和 IP 地址之间绑定关系的能力。图 4.8 中的交换机 A 和交换机 B 如果配置了 DHCP 侦听功能，在通过 DHCP 自动配置过程完成各个终端的网络信息配置后，构建了图 4.8 所示的 DHCP 配置表，配置表中内容通过侦听 DHCP 报文获得。当交换机通过非信任端口接收到 ARP 报文，用 ARP 报文中给出的 MAC 地址和 IP 地址对去匹配交换机中的 DHCP 配置表，如果匹配成功，则继续转发该 ARP 报文，否则，丢弃该 ARP 报文，这就是以太网交换机的防 ARP 欺骗攻击机制。

如果交换机 B 设置了防 ARP 欺骗攻击机制，当终端 B 发送图 4.9 所示的 ARP 报文时，由于交换机 B 连接终端 B 的端口是非信任端口，交换机 B 将用 MAC B 和 IP A 去匹配 DHCP 配置表，结果无法在交换机 B 的 DHCP 配置表中找到 MAC B 和 IP A 绑定在一起的项，交换机 B 将丢弃该 ARP 报文。

4.2　安全路由

Internet 是由多种不同类型的传输网络互联而成的互联网，而解决连接在不同类型的传输网络上的终端之间通信问题的关键是 IP，IP 为每一个终端分配统一的、与终端所连接的传输网络类型无关的 IP 地址，任何两个终端之间由 IP 路由协议建立 IP 层的传输路径，它由一系列路由器组成，同时，由 IP over X(X 指不同类型的传输网络)技术实现连接在同一个传输网络上的两个路由器之间或路由器和终端之间的 IP 分组传输过程。由此可以看出，路由协议是实现 IP 分组端到端传输的基础。虽然路由协议是基于 IP 的高层协议，但在由路由协议建立终端之间传输路径前，终端之间并不能实现端到端传输，因

此，IPSec 协议并不适合用于实现传输路由消息的两个端点之间的身份认证和路由消息的完整性检测，需要开发专用技术用于解决路由消息的正确传输问题。

4.2.1 路由器和路由项认证

图 4.10 是黑客实施路由欺骗攻击的过程，如果某个黑客想截获连接在局域网(Local Area Network，LAN)1 上终端发送给连接在 LAN 4 上终端的 IP 分组，通过接入 LAN 2 中的黑客终端发送一个以黑客终端 IP 地址为源地址、组播地址 224.0.0.9 为目的地址的路由消息，该路由消息伪造了一条黑客终端直接和 LAN 4 连接的路由项，路由器 R_1 和 R_2 均接收到该路由消息，对于路由器 R_1 而言，由于伪造路由项给出的到达 LAN 4 的距离最短，将通往 LAN 4 传输路径的下一跳路由器改为黑客终端，如图 4.10 中路由器 R_1 错误路由表所示，并导致路由器 R_1 将所有连接在 LAN 1 上终端发送给连接在 LAN 4 终端的 IP 分组错误转发给黑客终端。图 4.10 中终端 A 发送给终端 B 的 IP 分组，经过路由器 R_1 用错误的路由表转发后，不是转发给正确传输路径上的下一跳路由器 R_2，而是直接转发给黑客终端。

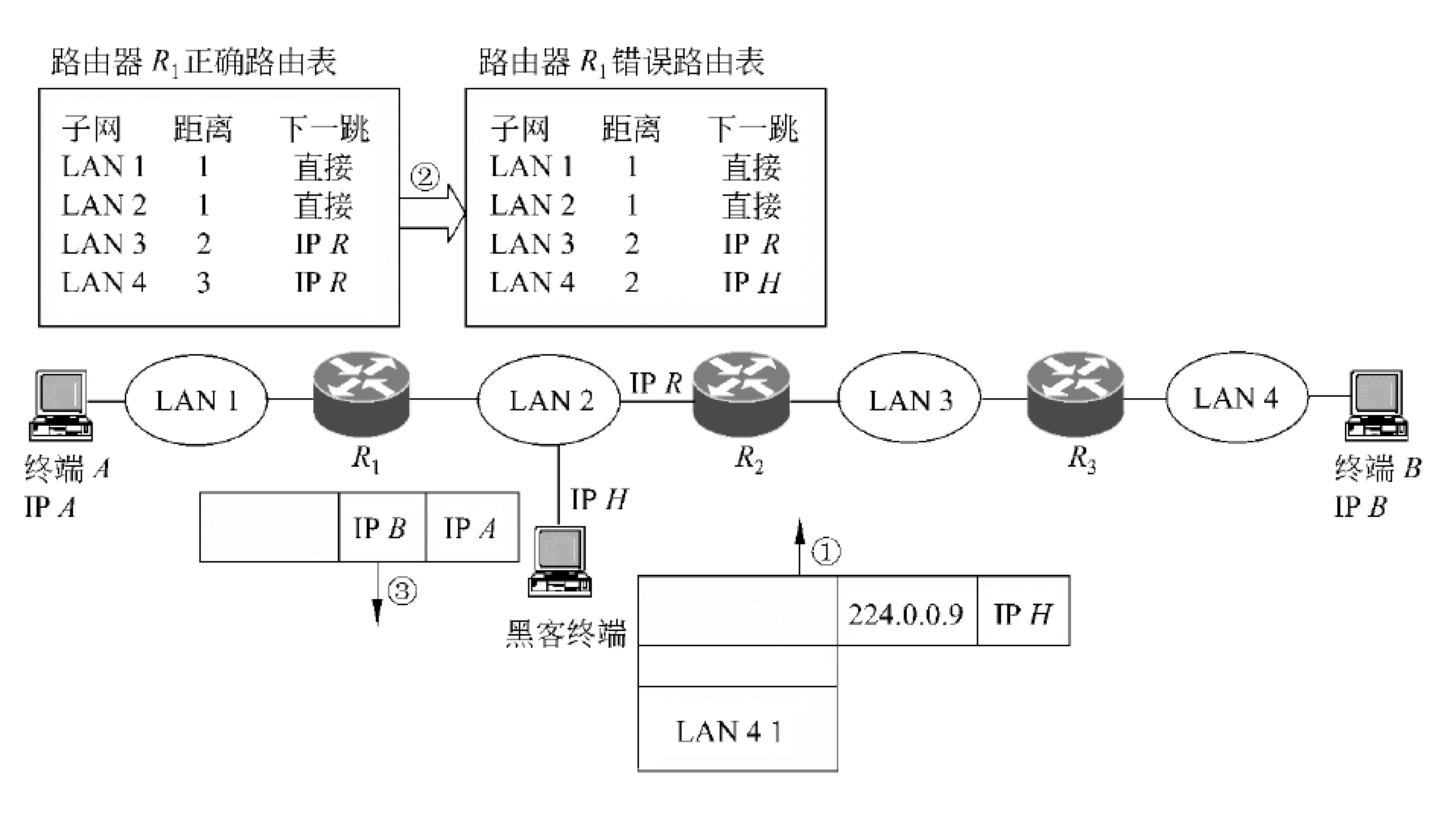


图 4.10 伪造路由过程

解决图 4.10 所示的路由欺骗攻击的机制是路由器和路由项认证，路由器接收到路由消息后，必须确认是合法路由器发送，且路由消息包含的路由项没有被篡改后，才对路由消息进行处理，并根据处理结果修改路由表。认证机制是在需要交换路由消息的路由器中配置共享密钥 K，如图 4.10 中的路由器 R_1 和 R_2 之间，R_2 和 R_3 之间，当某个路由器组播路由消息时，路由器根据路由消息和密钥 K 生成基于密钥的报文摘要，并将报文摘要附在路由消息后面一起组播给其他路由器，当某个路由器接收到路由消息，首先根据路由消息和密钥 K 计算基于密钥的报文摘要，然后将计算结果和附在路由消息后面的报文摘要比较，如果相同，表明发送者和接收者具有相同密钥，且路由消息在传输过程中没有被篡改，路由器对路由消息进行处理，整个过程如图 4.11 所示。

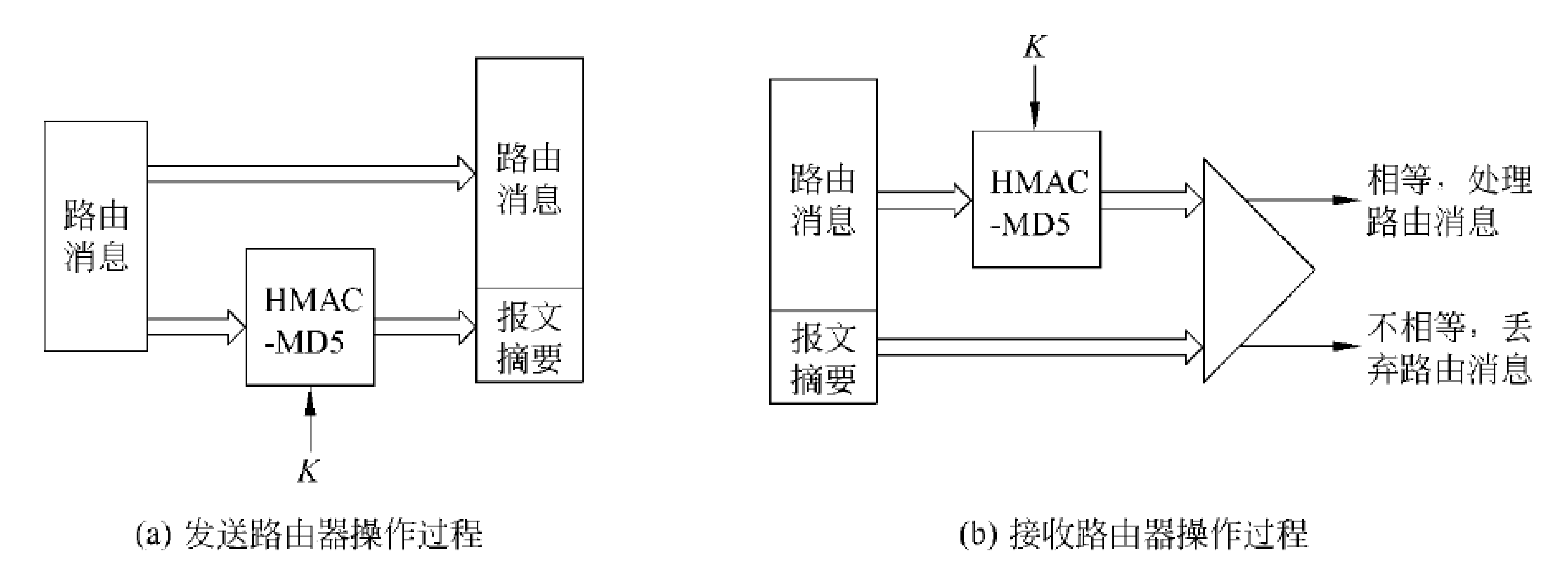


图 4.11　路由器和路由项认证过程

4.2.2　路由项过滤

如图 4.12 所示，路由器 R_1 连接了三个子网 192.168.1.0/24、192.168.2.0/24 和 193.7.1.0/24，但子网 192.168.1.0/24 和 192.168.2.0/24 属于内部子网，不能和外部网络中的终端通信，因此，对路由器 R_2 而言，这两个子网是不可见的，路由器 R_1 发送给路由器 R_2 的路由消息中不允许包含这两个子网对应的路由项，为此，需要在路由器 R_1 连接路由器 R_2 的端口配置路由项过滤器：192.168.0.0/22 过滤，当路由器 R_1 通过连接路由器 R_2 的端口组播路由消息时，路由消息中不允许包含目的网络地址和过滤器匹配的路由项，因此，路由器 R_1 通过连接路由器 R_2 的端口组播的路由消息中只包含路由项：193.7.1.0/24 1，路由器R_2 在路由表中只建立指明通往子网 193.7.1.0/24 的传输路径的路由项，对外部网络而言，子网 192.168.1.0/24 和 192.168.2.0/24 是不存在的。

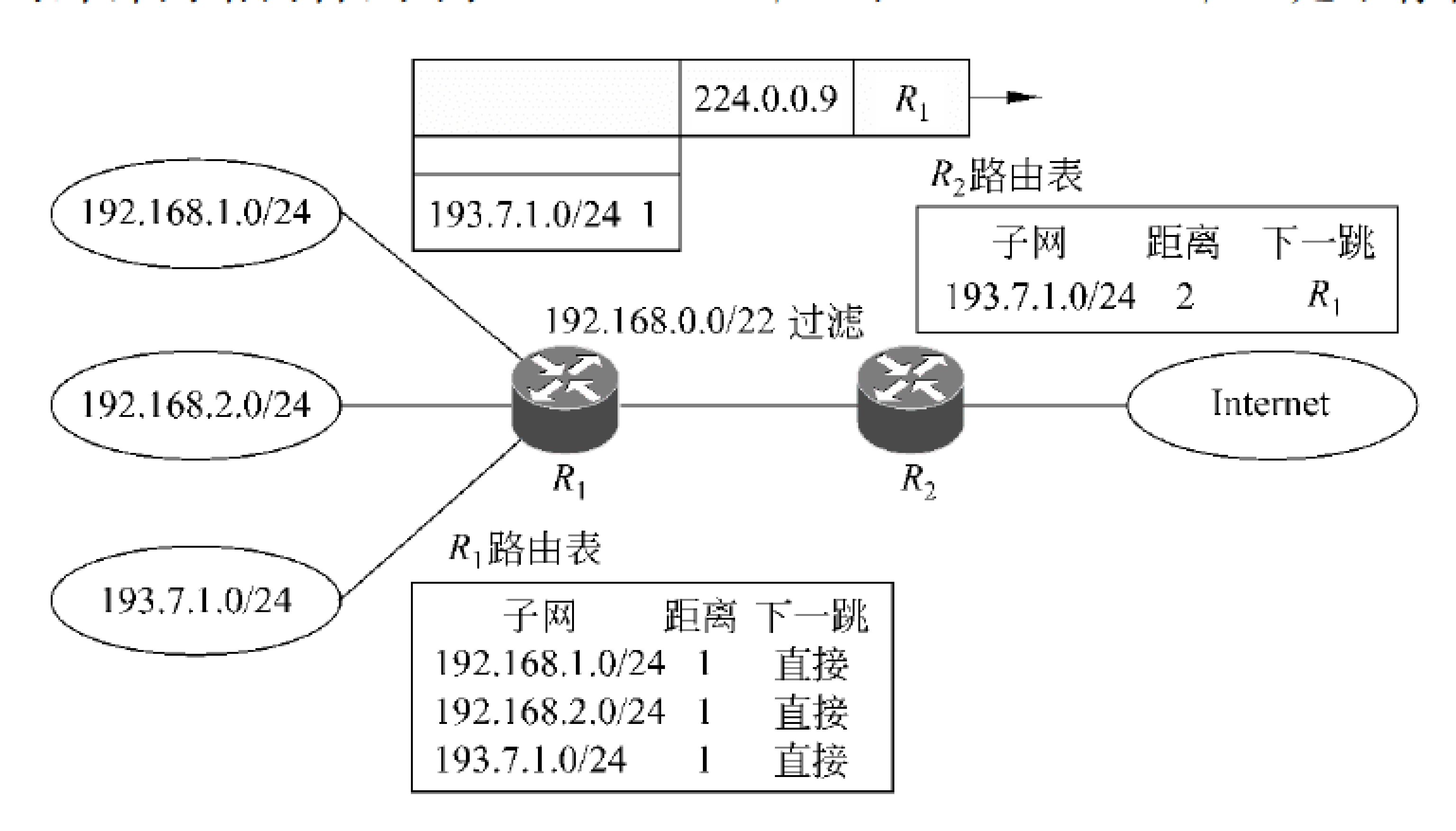
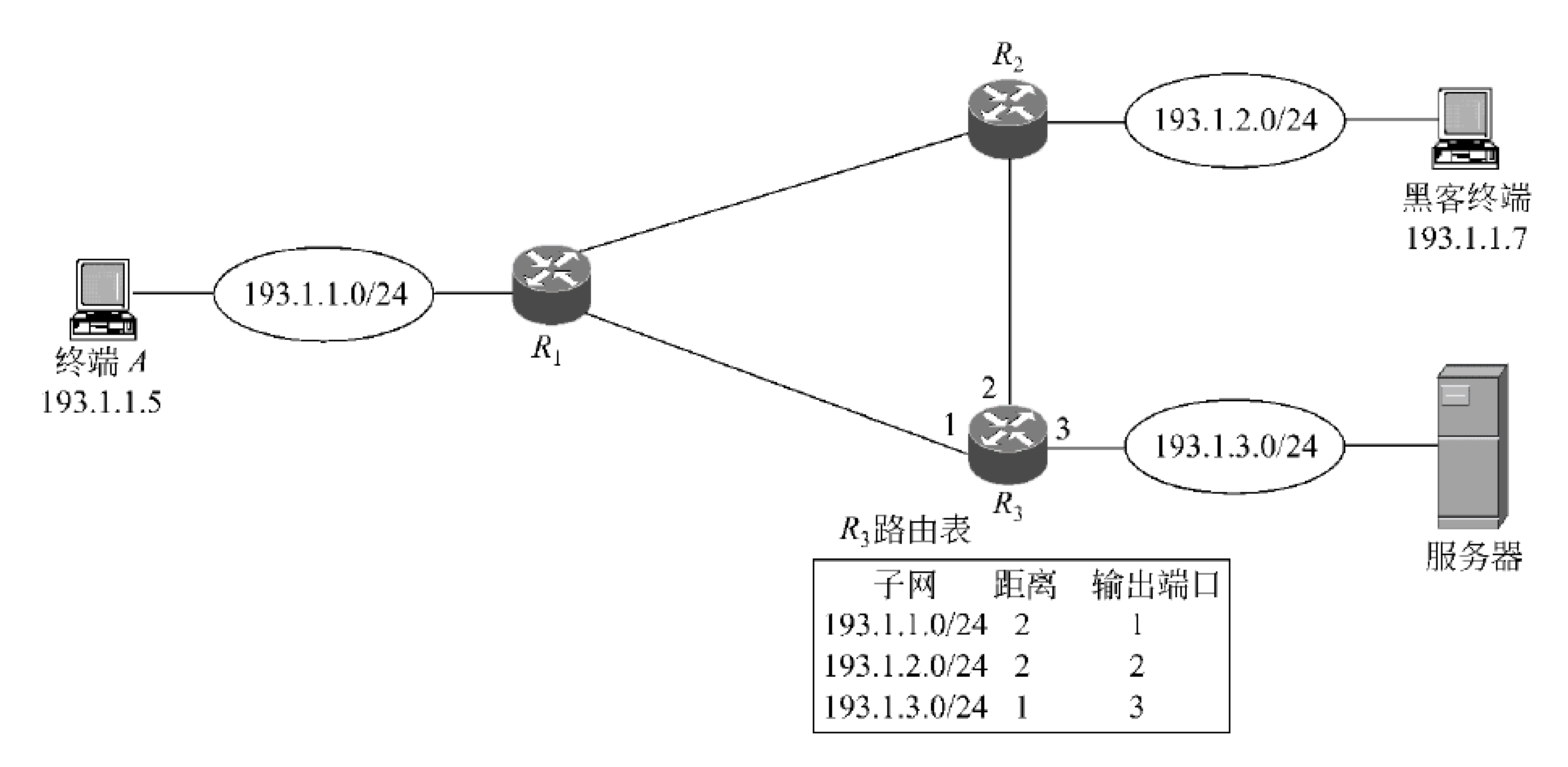


图 4.12　路由项过滤过程

4.2.3　单播反向路径验证

为了逃避追究，黑客终端发起攻击时，往往使用假的 IP 地址，如图 4.13 中的黑客终端，实际连接在子网 193.1.3.0/24 上，但冒用子网 193.1.1.0/24 的 IP 地址。这种冒用

IP 地址的攻击方式被称为源 IP 地址欺骗攻击。如果某个子网 NET1 至另一个子网 NET2 的传输路径和 NET2 至 NET1 的传输路径相同,则称 NET1 和 NET2 之间的路径为对称路径,网络中各个子网间的路径基本上为对称路径,如图 4.13 所示。对于由对称路径构成的网络,通过单播反向路径验证机制可以抑制源 IP 地址欺骗攻击。



子网	距离	输出端口
193.1.1.0/24	2	1
193.1.2.0/24	2	2
193.1.3.0/24	1	3

图 4.13 单播反向路径验证过程

当路由器从端口 X 接收到 IP 分组时,首先用该 IP 分组的源 IP 地址检索路由表,如果在路由表中找到匹配项,且该路由项指明的输出端口为 X,表明该 IP 分组的源 IP 地址不是伪造的,路由器继续该 IP 分组的转发处理,否则,确定该 IP 分组属于源 IP 地址欺骗攻击,路由器丢弃该 IP 分组,这就是单播反向路径验证过程。对于图 4.13 所示的网络,终端 A 发送给服务器的 IP 分组的源 IP 地址为 193.1.1.5,该 IP 分组经路由器 R_1 转发后,通过端口 1 进入路由器 R_3,路由器 R_3 首先用该 IP 分组的源 IP 地址 193.1.1.5 检索路由表,找到匹配项 193.1.1.0/24 2 1,确定路由项指明的输出端口和路由器 R_3 接收该 IP 分组的端口相同,都是端口 1,路由器 R_3 继续转发该 IP 分组。如果黑客终端冒用 IP 地址 193.1.1.7,黑客终端用于攻击服务器的 IP 分组经路由器 R_2 转发后,通过端口 2 进入路由器 R_3,路由器 R_3 首先用该 IP 分组的源 IP 地址 193.1.1.7 检索路由表,找到匹配项 193.1.1.0/24 2 1,确定路由项指明的输出端口为端口 1,和路由器 R_3 接收该 IP 分组的端口不同,路由器 R_3 确定该 IP 分组属于源 IP 地址欺骗攻击,路由器 R_3 丢弃该 IP 分组。

4.3 虚拟网络

虚拟网络是一种在同一个物理网络设施上构建多个逻辑上独立的网络的技术,图 4.14所示的就是在同一个物理网络设施上构建两个逻辑上独立的网络的过程。将一个物理网络设施划分为多个逻辑上独立的网络的目的是为了控制信息的传输过程,缩小黑客攻击的影响范围,因此,虚拟网络是一种目前常用的网络安全技术,计算机网络课程中详细讨论的虚拟局域网(Virtual LAN,VLAN)和虚拟专用网络(Virtual Private Network,VPN)技术就是典型的虚拟网络技术。

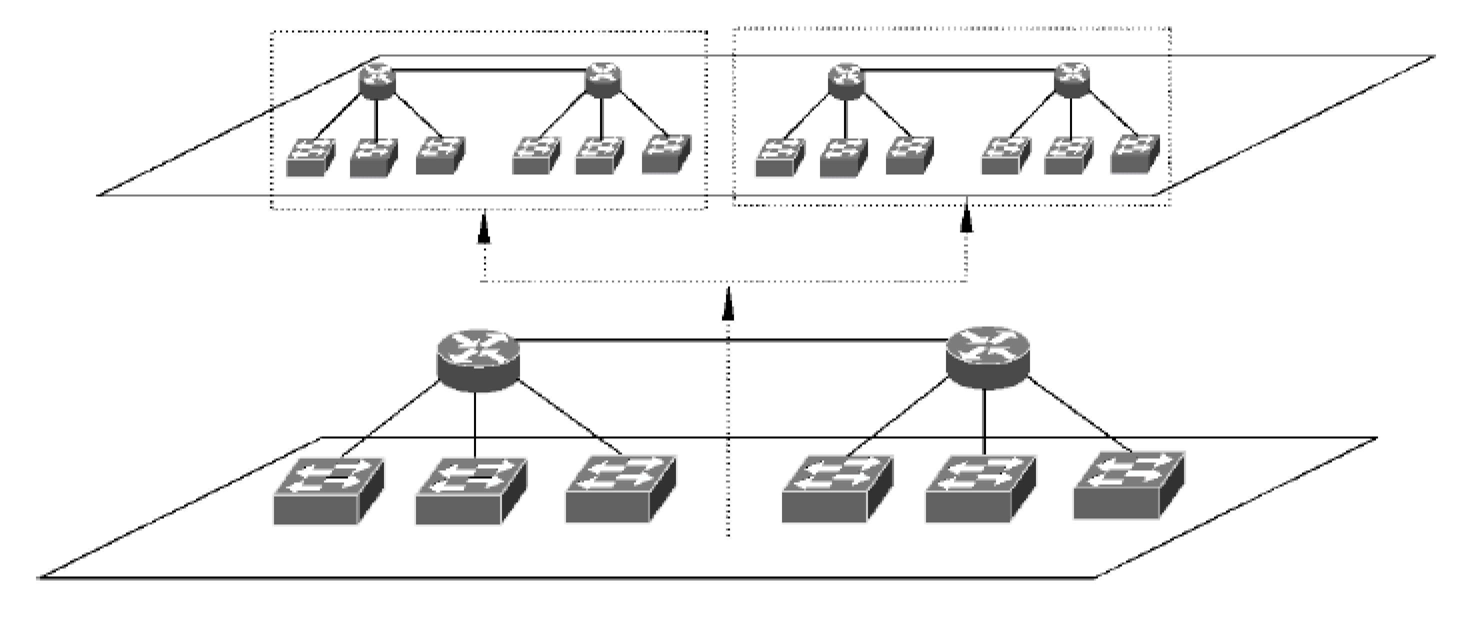


图 4.14　虚拟网络

4.3.1　虚拟局域网

1. 虚拟局域网安全机制

虚拟局域网技术可以将一个物理以太网划分为多个逻辑上完全独立的虚拟局域网(Virtual LAN,VLAN),即使两个终端连接在同一个物理以太网上,只要这两个终端不属于同一个 VLAN,这两个终端之间也不能通过以太网相互通信,所有的广播帧只能在同一个 VLAN 内广播,无法扩散到其他 VLAN。在前一节讨论 ARP 欺骗攻击时,黑客终端只能将属于同一个 VLAN 的终端的 IP 地址和自己的 MAC 地址绑定,因而也只能截获原本发送给同一个 VLAN 内的另一个终端的 IP 分组,根据不同的用户组成划分 VLAN,可以有效降低 ARP 欺骗攻击的危害(见图 4.15)。在划分 VLAN 后,以太网交换机提供的防站表溢出攻击、防 DHCP 欺骗攻击和防 ARP 欺骗攻击的机制都是针对某个 VLAN,而不是整个物理以太网。

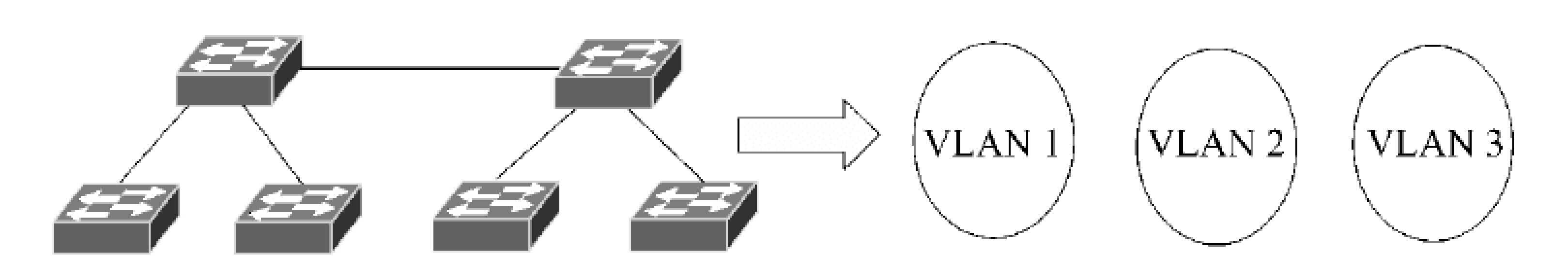


图 4.15　划分 VLAN 过程

2. 虚拟局域网安全应用实例

假定物理以太网结构如图 4.16 所示,为了安全,要求所有用于配置交换机的交换机 Web 接口和终端 *A* 属于一个 VLAN,属于其他 VLAN 的终端不允许访问该 VLAN,因此,该 VLAN 是一个不和其他 VLAN 连通的独立子网。为网络中的两个服务器单独划分 1 个 VLAN,网络中的其他终端单独划分 1 个 VLAN,允许除终端 *A* 以外的其他终端访问服务器,但需要由路由器对访问过程进行管制,网络中的交换机 S_7 是三层交换机,其他交换机为二层交换机,交换机通过属于默认 VLAN 的非标记端口访问 Web 接口。图 4.17是划分 VLAN 后的逻辑结构图,表 4.1 是各个 VLAN 的端口配置,VALN 1 的配置保证终端 *A* 能够访问到所有交换机的 Web 接口,VLAN 2 的配置保证除终端 *A* 以外的所有终端之间存在交换通路,同样,VLAN 3 的配置保证两个服务器之间存在交换通路。三层交换机 S_7 需要定义两个 IP 接口,分别对应 VLAN 2 和 VLAN 3,并需要分配 IP 地址 192.1.2.254 和 192.1.3.254。三层交换机的 IP 接口和路由表如图 4.17 所示。

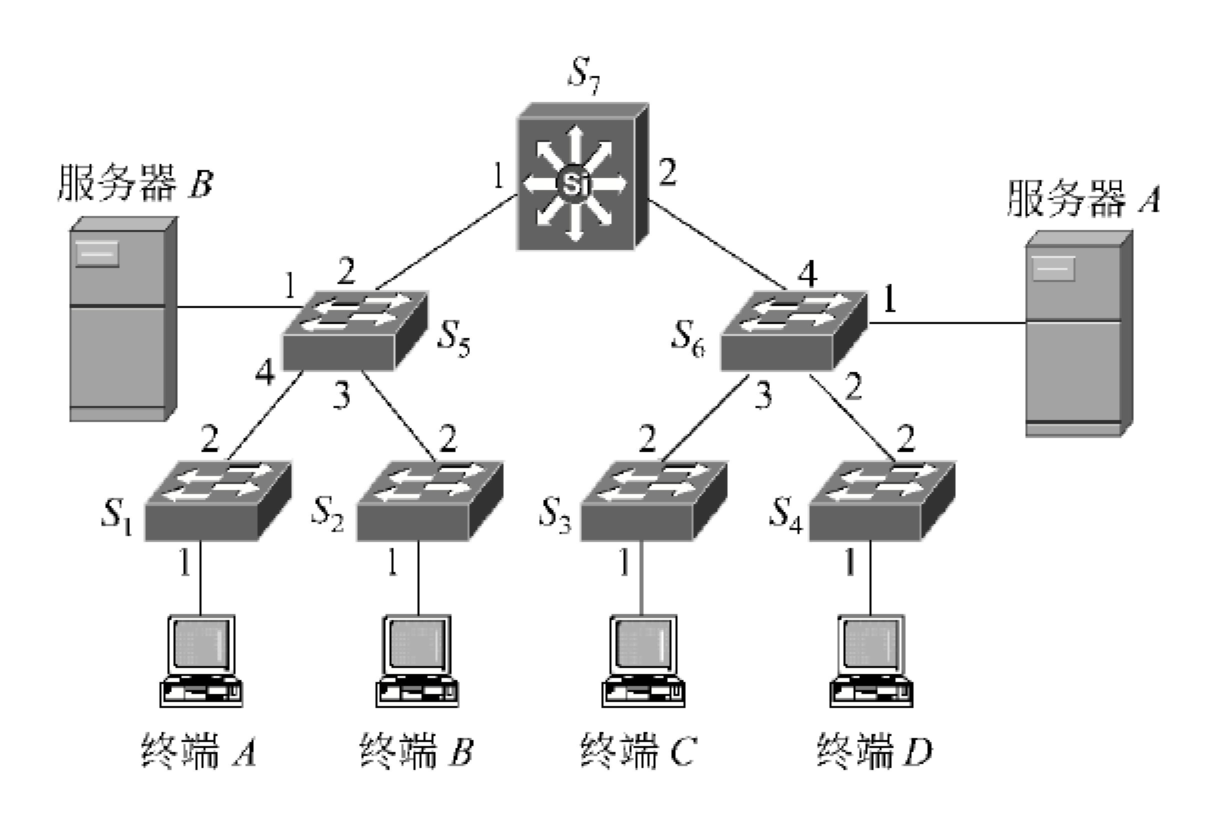


图 4.16 以太网网络结构二

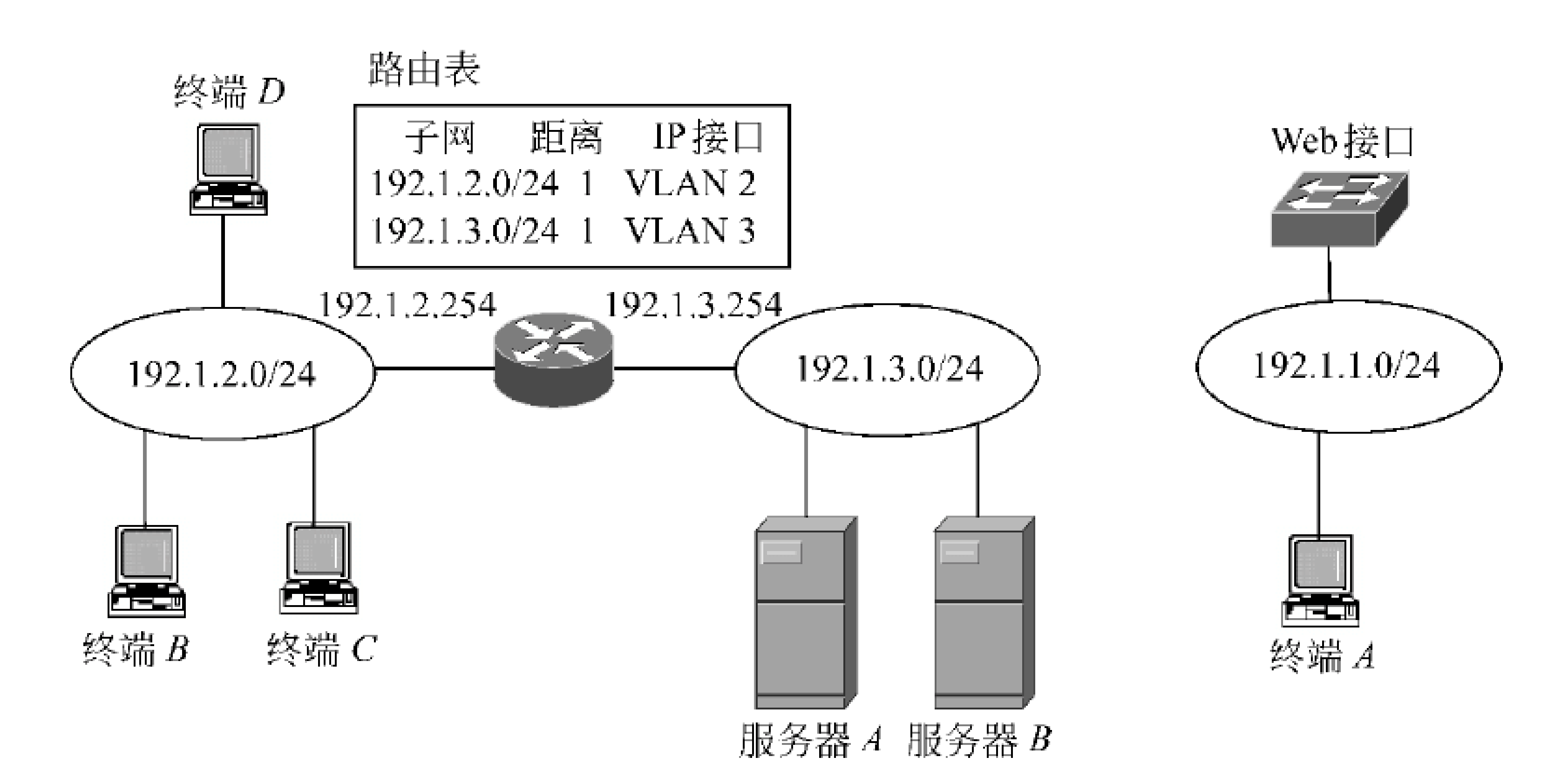


图 4.17 图 4.16 对应的逻辑结构

表 4.1 VLAN 端口配置表

VLAN	标 记 端 口	非标记端口
VLAN 1		$S_{1.1}$、$S_{1.2}$、$S_{5.4}$、$S_{5.3}$、$S_{5.2}$、$S_{2.2}$、$S_{7.1}$、$S_{7.2}$、$S_{6.4}$、$S_{6.3}$、$S_{6.2}$、$S_{3.2}$、$S_{4.2}$
VLAN 2	$S_{2.2}$、$S_{5.3}$、$S_{5.2}$、$S_{7.1}$、$S_{7.2}$、$S_{6.4}$、$S_{6.3}$、$S_{6.2}$、$S_{3.2}$、$S_{4.2}$	$S_{2.1}$、$S_{3.1}$、$S_{4.1}$
VLAN 3	$S_{5.2}$、$S_{7.1}$、$S_{7.2}$、$S_{6.4}$	$S_{5.1}$、$S_{6.1}$

注：$S_{1.1}$表示交换机 S_1 的端口 1。

4.3.2 虚拟路由器

1. 虚拟路由器安全机制

虚拟局域网技术可以把一个物理以太网划分为多个 VLAN，每一个 VLAN 都是逻辑上独立的局域网。路由器是互连不同类型传输网络的互连设备，虚拟路由器(Virtual Router，VR)技术可以将一个物理路由器分解为多个逻辑上完全独立的虚拟路由器，每一

个虚拟路由器的功能等同于传统的物理路由器，有独立的接口、执行路由协议的路由进程和路由表，当然，多个虚拟路由器的逻辑接口可能共享物理路由器的单个物理接口。虚拟路由器和虚拟局域网结合，可以将一个物理互联网分解为多个完全独立的逻辑互联网，逻辑互联网之间不能直接通信(见图 4.18)。目前许多企业构建两套内部网，一套内部网不和 Internet 互联，只允许内部终端访问内部的数据库服务器，另一套内部网络允许和 Internet 互联，并且允许外部网络终端访问企业的 Web 服务器等，这两套内部网络逻辑上必须完全独立，以免发生外部黑客攻击内部数据库服务器的事件。当然，分别构建两套物理上完全独立的内部网络是最安全的解决方法，一些有特殊安全要求的单位也是这样做的，但这样做一是提高了网络建设成本，二是降低了终端配置的灵活性，只有通过改变物理连接才能将某个终端从一个内部网络转移到另一个内部网络。

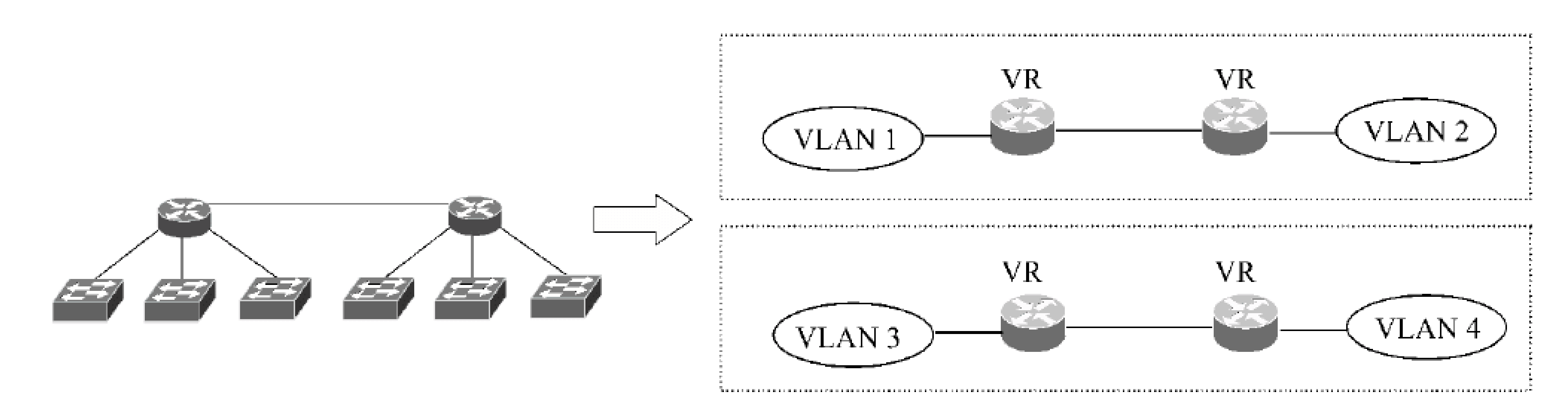


图 4.18　虚拟路由器生成多个独立网络过程

2. 虚拟路由器安全应用实例

图 4.19 是内部网络的物理结构，图 4.20 是逻辑上完全独立的两套内部网络，其中一套内部网络中的终端与服务器和 Internet 完全隔离，另一套内部网络中的终端与服务器允许和 Internet 相互交换数据。为实现这一点，需要将路由器 R_1 和 R_2 分别分解成两个虚拟路由器 VR1.1、VR1.2 和 VR2.1、VR2.2。同时分别为每一个虚拟路由器定义 IP 接口、路由协议等。如果属于同一个物理路由器的两个虚拟路由器共享某个物理端口，必须为进出这种共享端口的数据设置用于区别该数据所属虚拟路由器的标记，在以太网中，最适合用作标记的信息是 VLAN ID，因此，如果某个共享端口分别定义了两个属于不同虚拟路由器的 IP 接口，这两个 IP 接口必须属于不同的 VLAN，而且该共享端口必须为标记

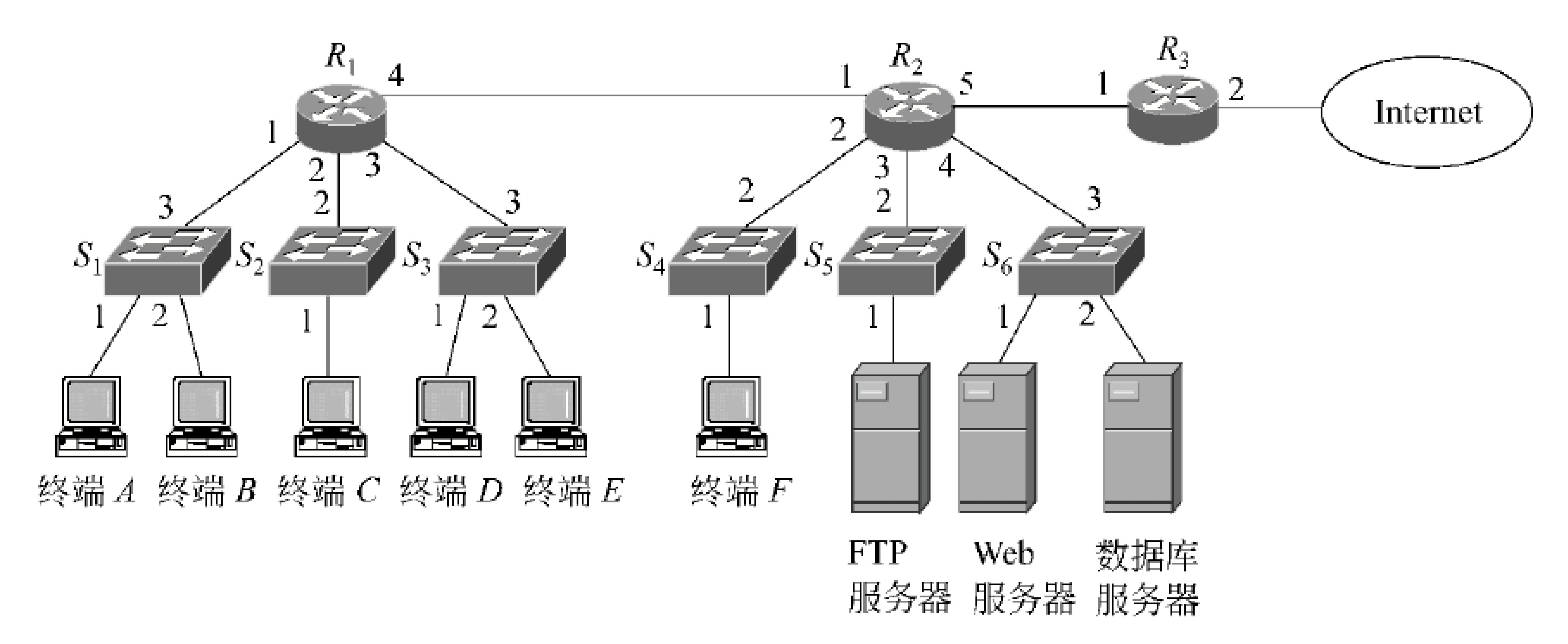
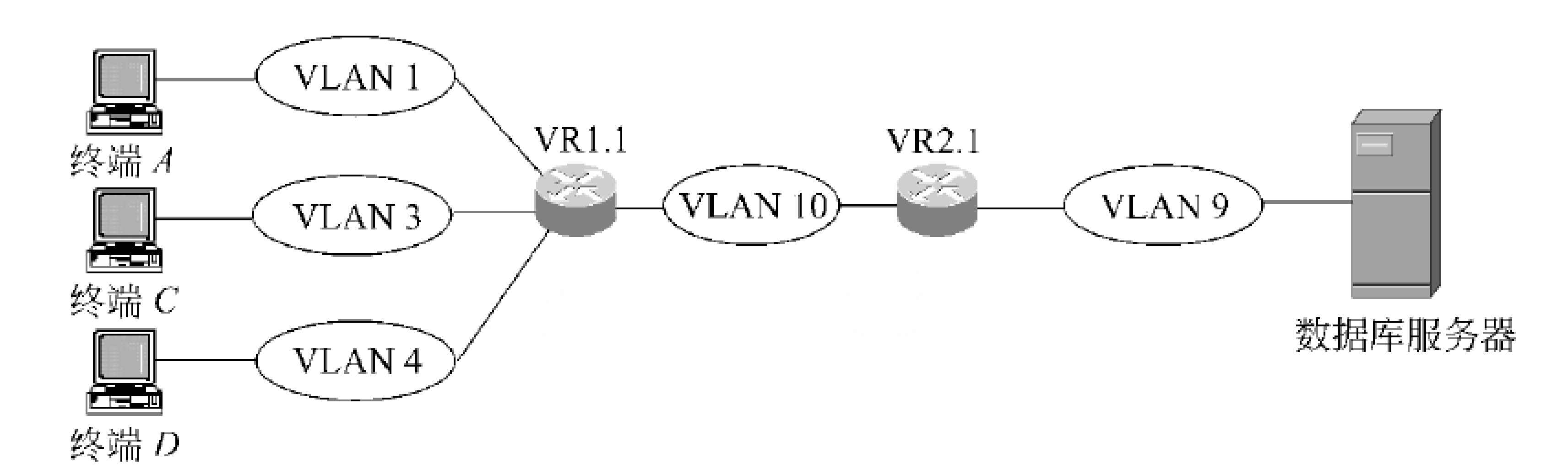
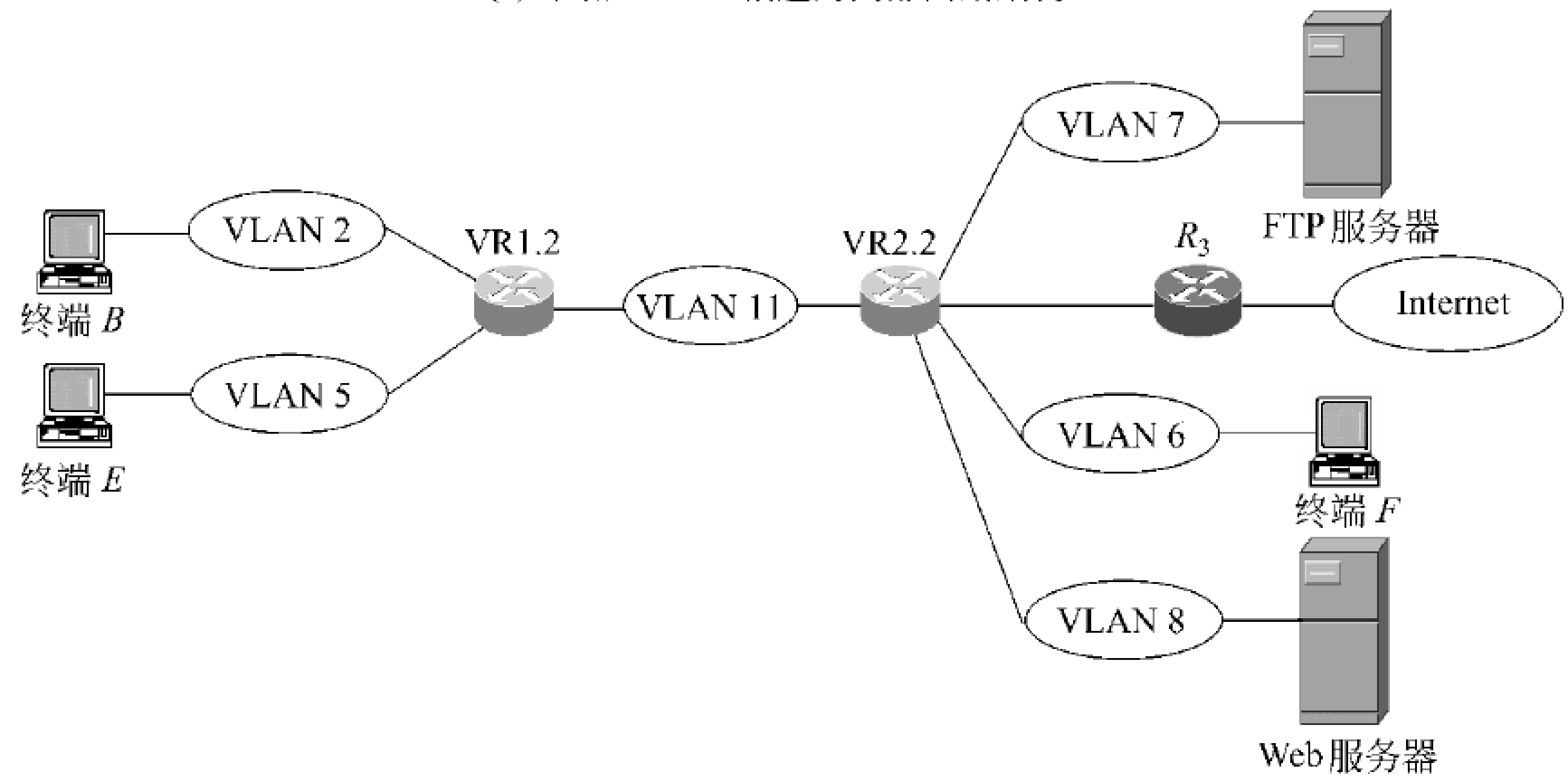


图 4.19　内部网络物理结构图

端口，进出该共享端口的数据携带用于标识所属 IP 接口的 VLAN ID。表 4.2 给出了各个 VLAN 的端口配置，$R_{1.1}$表示物理路由器 R_1 的端口 1。




(a) 不和 Internet 相连的内部网络结构



(b) 和 Internet 相连的内部网络结构

图 4.20　内部网络逻辑结构图

表 4.2　VLAN 端口配置表

VLAN	标　记　端　口	非标记端口
VLAN 1	$S_{1.3}$、$R_{1.1}$	$S_{1.1}$
VLAN 2	$S_{1.3}$、$R_{1.1}$	$S_{1.2}$
VLAN 3		$S_{2.1}$、$S_{2.2}$、$R_{1.2}$
VLAN 4	$S_{3.3}$、$R_{1.3}$	$S_{3.1}$
VLAN 5	$S_{3.3}$、$R_{1.3}$	$S_{3.2}$
VLAN 6		$S_{4.1}$、$S_{4.2}$、$R_{2.2}$
VLAN 7		$S_{5.1}$、$S_{5.2}$、$R_{2.3}$
VLAN 8	$S_{6.3}$、$R_{2.4}$	$S_{6.1}$
VLAN 9	$S_{6.3}$、$R_{2.4}$	$S_{6.2}$
VLAN 10	$R_{1.4}$、$R_{2.1}$	
VLAN 11	$R_{1.4}$、$R_{2.1}$	

注：$R_{1.1}$表示路由器 R_1 的端口 1。

假定 VALN 1～VLAN 9 对应的子网地址为 192.1.1.0/24～192.1.9.0/24，虚拟路由器对应的路由表如表 4.3～表 4.6 所示，通过属于不同虚拟路由器的 IP 接口进入的 IP 分组被提交给对应的路由进程，对应的路由进程检索属于自己的路由表，通过属于自己的 IP 接口转发 IP 分组，因此，属于某个内部网络的 IP 分组，无法进入另一个内部网络。

表 4.3　VR1.1 路由表

子　网	距　离	输出端口	VLAN	下一跳
192.1.1.0/24	1	1	VLAN 1	直接
192.1.3.0/24	1	2		直接
192.1.4.0/24	1	3	VLAN 4	直接
192.1.9.0/24	2	4	VLAN 10	VR2.1

表 4.4　VR2.1 路由表

子　网	距　离	输出端口	VLAN	下一跳
192.1.1.0/24	2	1	VLAN 10	VR1.1
192.1.3.0/24	2	1	VLAN 10	VR1.1
192.1.4.0/24	2	1	VLAN 10	VR1.1
192.1.9.0/24	1	4	VLAN 9	直接

表 4.5　VR1.2 路由表

子　网	距　离	输出端口	VLAN	下一跳
192.1.2.0/24	1	1	VLAN 2	直接
192.1.5.0/24	1	3	VLAN 5	直接
192.1.6.0/24	2	4	VLAN 11	VR2.2
192.1.7.0/24	2	4	VLAN 11	VR2.2
192.1.8.0/24	2	4	VLAN 11	VR2.2
0.0.0.0/0		4	VLAN 11	VR2.2

表 4.6　VR2.2 路由表

子　网	距　离	输出端口	VLAN	下一跳
192.1.2.0/24	2	1	VLAN 11	VR1.2
192.1.5.0/24	2	1	VLAN 11	VR1.2
192.1.6.0/24	1	2		直接
192.1.7.0/24	1	3		直接
192.1.8.0/24	1	4	VLAN 8	直接
0.0.0.0/0		5		R_3

4.3.3 虚拟专用网

虚拟专用网(Virtual Private Network,VPN)是一种通过共享的分组交换网络实现各子网间互联,但其安全性又与通过点对点专用链路实现各子网间互联的专用网络一样的联网技术,从虚拟网络角度看,VPN 主要采用了虚拟路由器和虚拟点对点路径的技术。图 4.21 给出了用 MPLS 网络实现专用网络 VPN *A* 和 VPN *B* 各子网间互联的物理结构,图 4.22 给出了采用虚拟路由器和虚拟点对点路径实现 VPN 的逻辑结构,图 4.22 中,MPLS 域建立 PE1 和 PE2 之间的双向标签交换路径(Label Switched Path,LSP),这两条 LSP 就像点对点链路,用于互连 PE1 和 PE2。PE1 和 PE2 被分解为两个虚拟路由器,分别用于连接 VPN *A* 和 VPN *B*,由于 PE1 和 PE2 通过单独的端口连接 VPN *A* 和 VPN *B*,因此,通过连接 CE 的端口可以确定发送数据的 VPN,但由于两个 PE 之间的 LSP 被两个 VPN 共享,因此,当某个 PE 通过 LSP 接收到数据时,数据必须携带用于让 PE 确定转发该数据的虚拟路由器的标记,在 MPLS 中,用 VPN 标签标识数据所属的 VPN,当某个 PE 通过 LSP 向另一个 PE 发送数据时,数据必须携带标识数据所属的 VPN 的 VPN 标签。图 4.23 给出了 CE1 至 CE3 的 IP 分组传输过程。VPN 是一种非常普遍的安全网络技术,将在第 6 章作完整介绍。

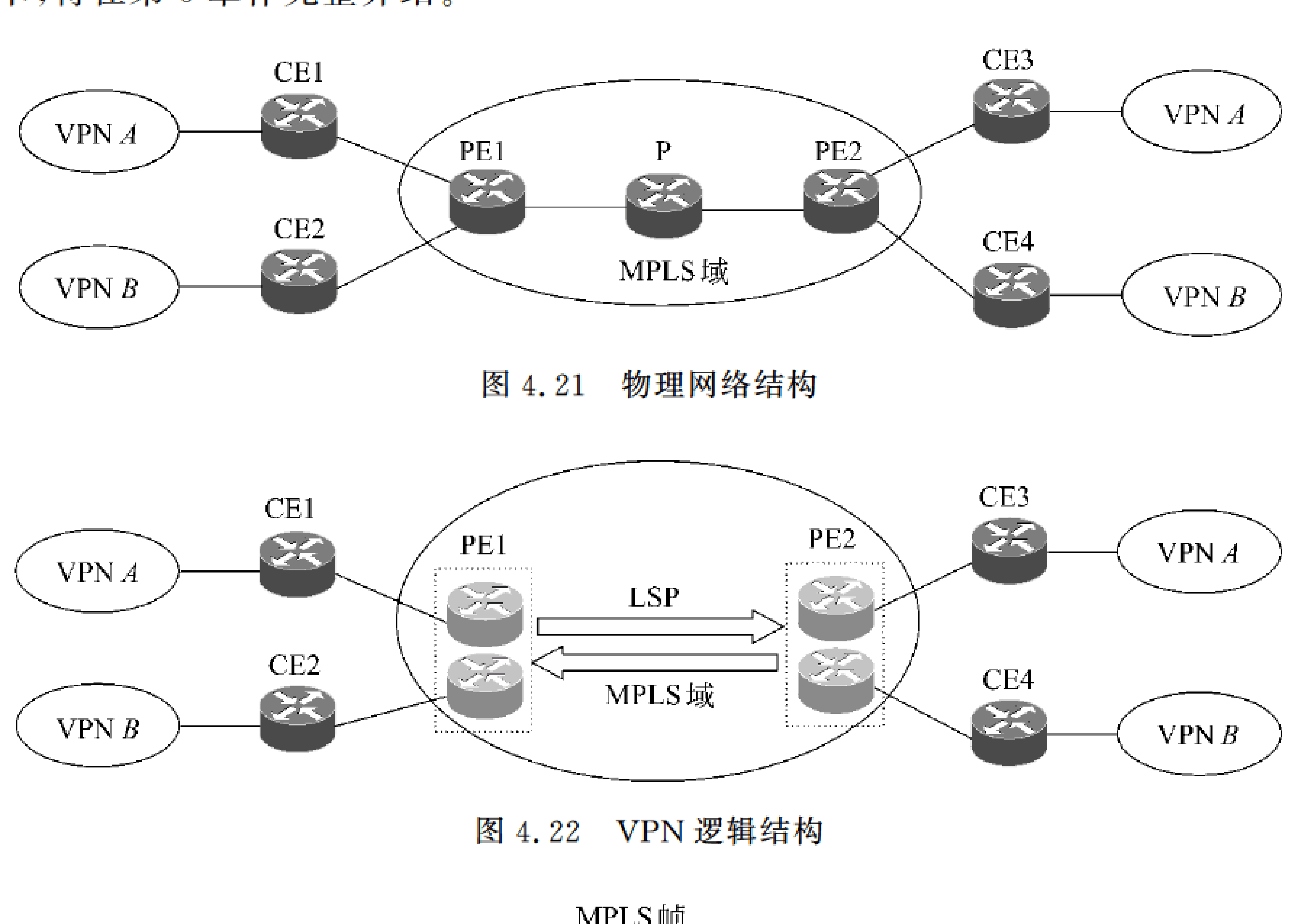


图 4.21 物理网络结构

图 4.22 VPN 逻辑结构

MPLS 帧

LSP 标签
VPN 标签
IP 分组

IP 分组

IP 分组

CE1 PE1 LSP PE2 CE3

图 4.23 CE1 至 CE3 IP 分组传输过程

4.4　信息流管制

图 4.24 是 SYN 泛洪攻击过程，黑客终端伪造多个本不存在的 IP 地址，请求和 Web 服务器建立 TCP 连接，服务器在接收到 SYN=1 的建立连接请求后，为请求建立的连接分配资源，并发送 SYN=1、ACK=1 的确认响应。但由于黑客终端是用伪造的 IP 地址发起的 TCP 连接建立过程，服务器发送的确认响应不可能到达真正的网络终端，因此，也无法接收到来自客户端的确认报文，该 TCP 连接处于未完成状态，分配的资源被闲置。

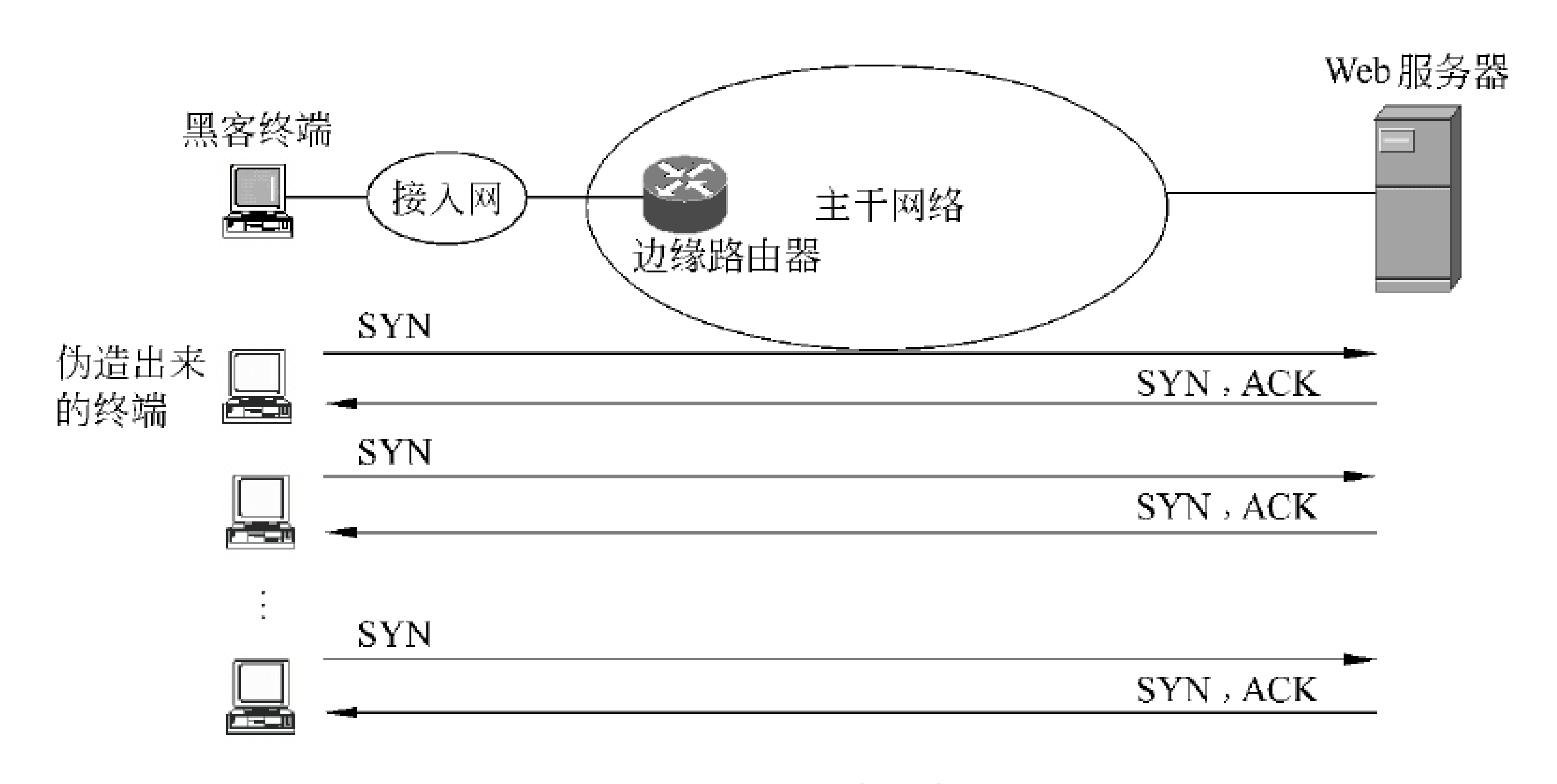


图 4.24　SYN 泛洪攻击过程

图 4.25 是分布式拒绝服务攻击(DDOS)过程，多个黑客终端同时向 Web 服务器发送大量的 ICMP ECHO 请求报文，导致主干网络中通往 Web 服务器的路径被拥塞，Web 服务器的处理能力被大量 ICMP ECHO 请求报文消耗，无法提供正常的 Web 服务功能。

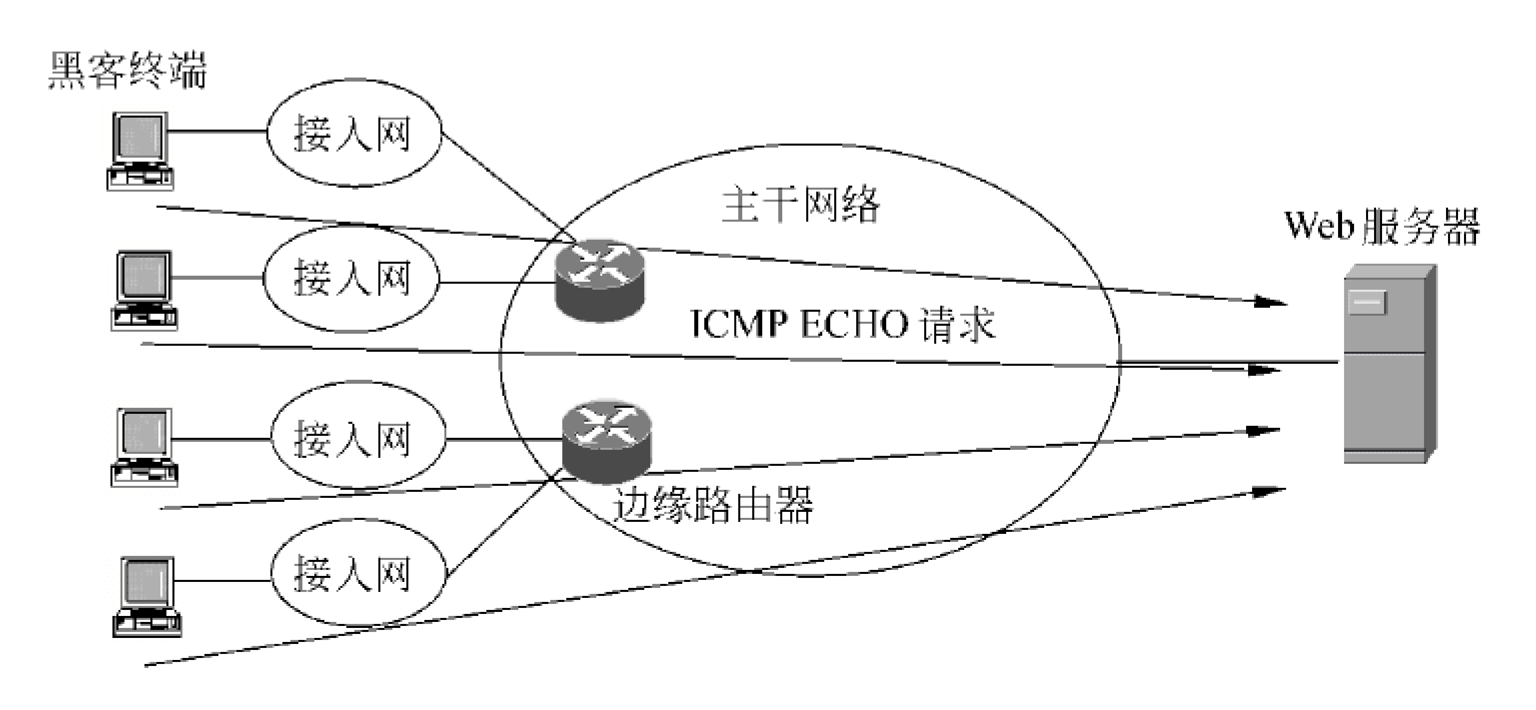


图 4.25　分布式拒绝服务攻击(DDOS)过程

拒绝服务攻击的共同点是黑客终端向被攻击者超量发送报文，因此，只要能够限制某类报文的流量，就能够抑制拒绝服务攻击。在 Internet 中，所有终端都通过接入网络接入 Internet，Internet 主干网中用于连接接入网络的路由器称为边缘路由器，如果边缘路由

器能够对通过接入网络输入的信息流量进行管制，不仅能够有效控制 Internet 主干网中的信息流量，避免发生拥塞，而且还能够有效抑制拒绝服务攻击。

4.4.1 信息流分类

信息流分类是要从 IP 分组流中分离出属于特定应用的一组 IP 分组，如需要分离出建立 TCP 连接过程中的第一个请求报文，需要从 IP 分组流中分离出具有如下特征的 IP 分组。

- IP 首部协议字段值：6(TCP)。
- TCP 首部控制标志位：SYN=1，ACK=0。

上述用于分离出特定 IP 分组的特征信息组合就是 IP 分组的分类标准。以下就是分类 ICMP ECHO 请求报文的分类标准。

- IP 首部协议字段值：1(ICMP)。
- ICMP 类型字段值：8(ECHO 请求)。

4.4.2 管制算法

信息流管制是一种将属于特定应用的 IP 分组的传输速率限定在某个设定值的技术，由于数据通信存在突发性和间歇性，因此，需要有适应突发性和间歇性的管制算法，漏斗算法将信息流限制在一个设定的传输速率，令牌桶算法在限制平均传输速率的前提下，允许短暂的超过平均速率的突发速率。

1. 漏斗算法

漏斗如图 4.26 所示，不管物体进入漏斗的速率是多少，也不管漏斗中有多少物体，漏斗出口总是恒速输出物体。当然，一旦漏斗装满物体，后续物体将被丢弃。将漏斗工作原理用于限速用户进入网络的信息流的过程如图 4.27 所示，突发性信息流首先存入缓冲器，如果缓冲器满，则丢弃后续的 IP 分组，队列稳定器就像漏斗出口，恒速输出信息流。这样，虽然用户信息流进入边缘路由器的速率是随机的，但通过边缘路由器进入网络的速率是恒定的，达到了限速用户信息流的目的。图 4.27 中队列缓冲器的长度确定了 IP 分组由于信息流整形而导致的时延大小。

图 4.26 漏斗

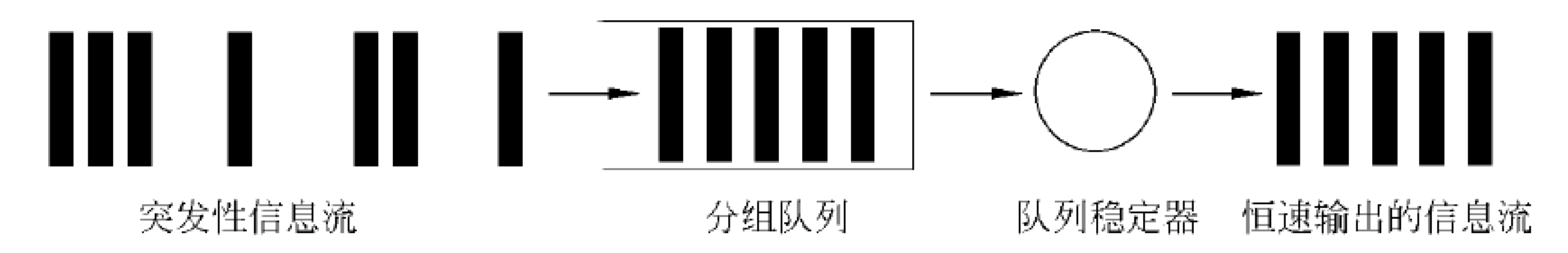


图 4.27 用漏斗算法限速信息流的过程

2. 令牌桶算法

漏斗算法保证用户信息流恒速进入网络，但大多数情况下，对用户进行的流量管制主要在于限制用户信息流进入网络的平均速率，短暂的超速信息流是允许的，而且也符合数

据通信的突发性、间隙性特征。因此,需要一种允许短暂超速、但又能对平均速率进行管制的限速算法,它就是令牌桶算法。令牌桶速率限制算法限制长期平均传输速率,允许有限制的突发性信息流进入网络。在这种方法中,令牌桶用作管理、控制 IP 分组进入网络的速率的调节器,图 4.28 给出了这种速率管制算法的操作过程。

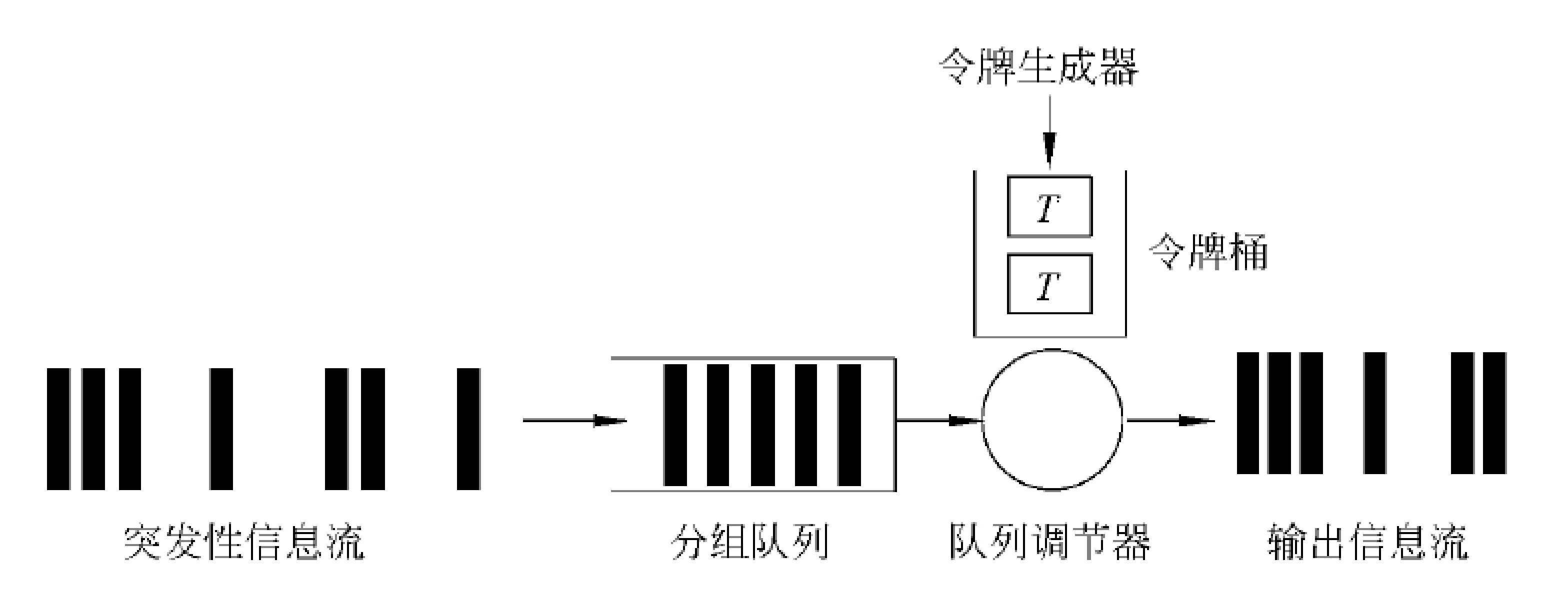


图 4.28 令牌桶算法操作过程

令牌生成器以每秒 R 令牌的速率产生令牌,并将它们放入具有 D 个令牌深度的令牌桶。每一个令牌授予传输固定数量字节的能力,当令牌桶装满 D 个令牌时,丢弃新产生的令牌。在令牌生成器产生令牌的同时,突发性 IP 分组流到达并被放入长度为 L 的分组队列中,当 IP 分组流量超出分组队列能够存储的容量时,将丢弃多余的 IP 分组。

队列调节器确定转发一个具有 P 个令牌所对应的字节长度的 IP 分组时的算法如下:如果令牌桶中包含了 T 个令牌,当 P 小于等于 T 时,IP 分组立即送入网络,并从令牌桶中移走 P 个令牌。如果 P 大于 T,IP 分组必须在队列中等待,直到令牌桶中拥有 P 个令牌时,IP 分组才能送入网络,并从令牌桶中移走 P 个令牌。

令牌桶速率限制算法既可以调节用户信息流的平均传输速率,又允许一定流量、一定持续时间的突发性信息流进入网络。令牌生成器产生令牌的速率确定了信息流的平均速率,令牌桶的深度确定了突发性信息流的最大流量,队列长度限制了 IP 分组由于信息流整形而导致的时延大小。

4.4.3 信息流管制抑制拒绝服务攻击机制

图 4.29 是一个简化了的校园网结构,它由核心层、汇聚层和接入层交换机组成,接入层交换机完成用户终端的接入,汇聚层交换机完成用户身份认证和信息流管制,核心层交换机完成 IP 分组的线速转发。从功能划分看,主要的管理和控制功能由汇聚层实现,核心层的主要任务是完成 IP 分组的线速转发。这样的校园网结构常常因为某个感染病毒的用户终端所发起的拒绝服务攻击,使网络服务处于瘫痪状态。因此,必须尽量控制某个感染病毒的用户终端的影响范围,为此,根据用户终端的组成,将用户终端分成若干个 VLAN,汇聚层交换机成为这些 VLAN 接入核心层的边缘路由器。划分 VLAN 后的网络结构如图 4.30 所示,VLAN 终端配置如表 4.7 所示,为抑制用户终端发起的拒绝服务攻击,必须在汇聚层交换机连接由用户终端组成的 VLAN 的 VLAN 接口设置信息流管

制器,信息流管制器由两部分组成,一是用于定义需要管制的信息流类型的分类标准,二是分类标准所定义的信息流的速率限制。速率限制由平均传输速率和突发性数据长度给出,平均传输速率确定图 4.28 中的令牌生成速率,突发性数据长度确定令牌桶的深度。假定平均传输速率为 64Kb/s,突发性数据长度为 8000B,每一个令牌 P 代表 100b,则可求出令牌生成速率=(64Kb/s)/100=640 个/s,令牌桶深度=(8000×8)/100=640 个令牌。为了有效抑制 SYN 泛洪攻击和大量发送 ICMP ECHO 请求或响应的分布式拒绝服务攻击,在所有汇聚层交换机连接由用户终端组成的 VLAN 的 VLAN 接口设置如下信息流管制器。

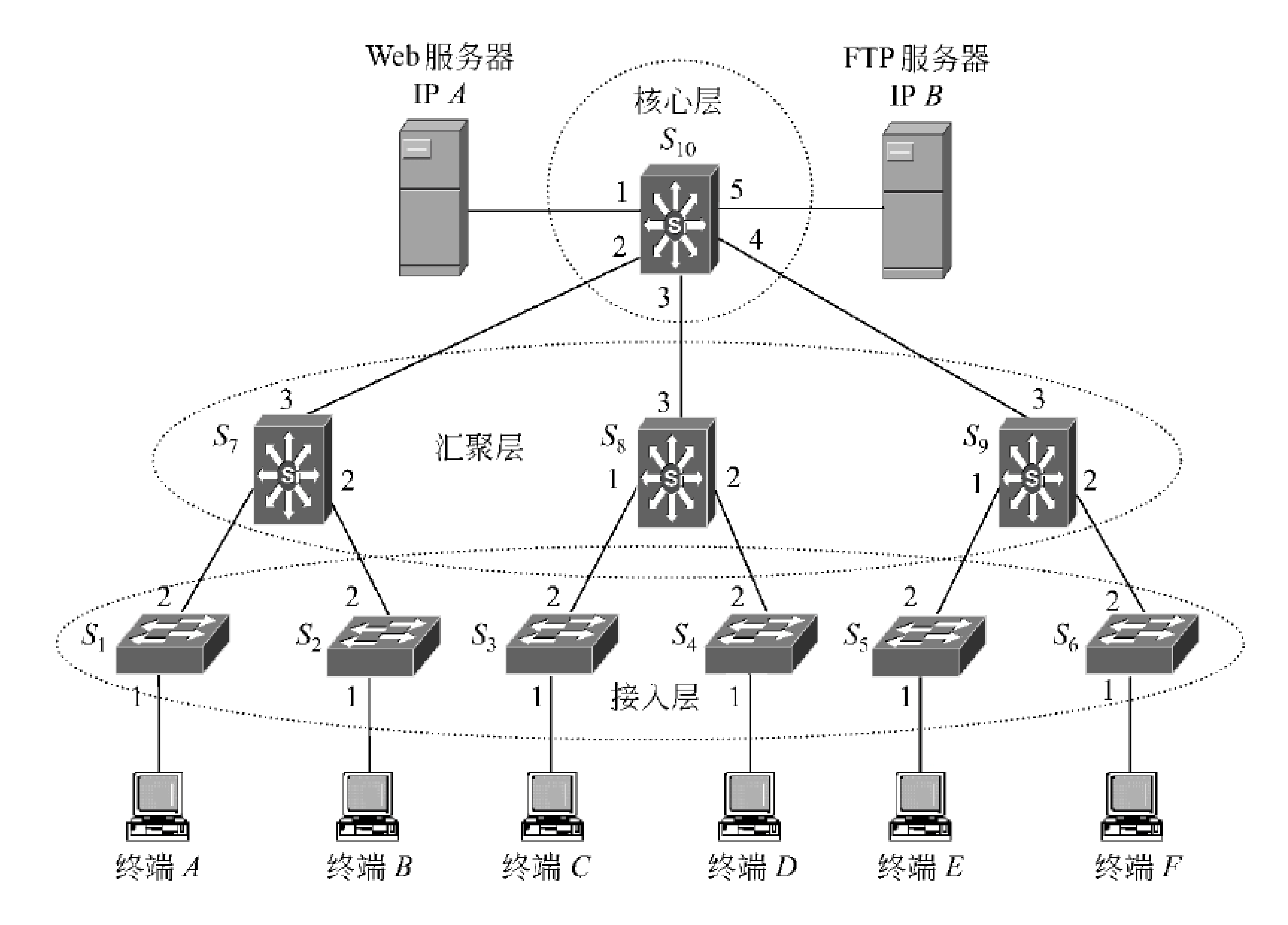


图 4.29　校园网物理结构图

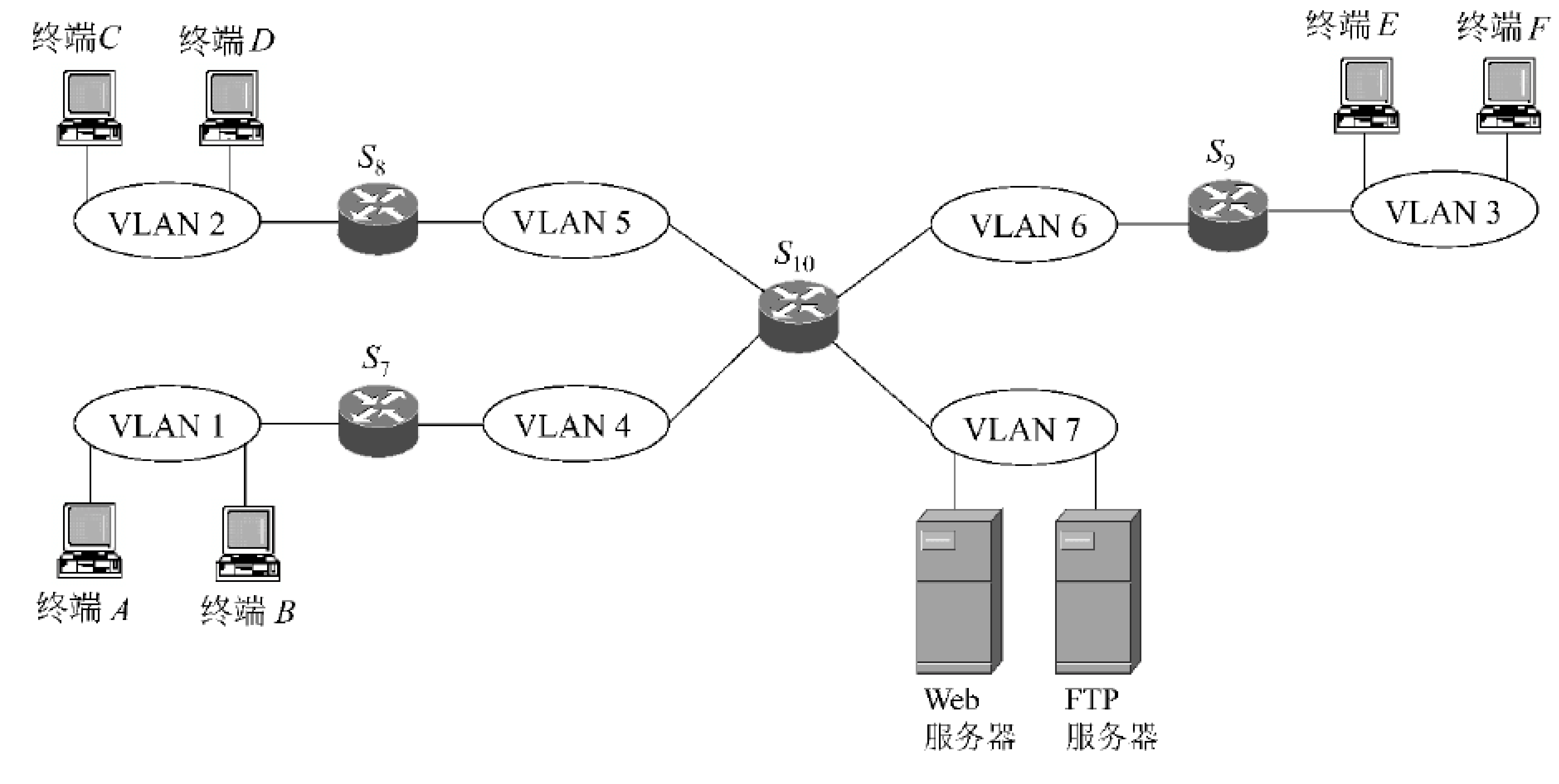


图 4.30　校园网逻辑结构图

表 4.7　VLAN 端口配置表

VLAN	标 记 端 口	非标记端口
VLAN 1		$S_{1.1}$、$S_{1.2}$、$S_{2.1}$、$S_{2.2}$、$S_{7.1}$、$S_{7.2}$
VLAN 2		$S_{3.1}$、$S_{3.2}$、$S_{4.1}$、$S_{4.2}$、$S_{8.1}$、$S_{8.2}$
VLAN 3		$S_{5.1}$、$S_{5.2}$、$S_{6.1}$、$S_{6.2}$、$S_{9.1}$、$S_{9.2}$
VLAN 4		$S_{7.3}$、$S_{10.2}$
VLAN 5		$S_{8.3}$、$S_{10.3}$
VLAN 6		$S_{9.3}$、$S_{10.4}$
VLAN 7		$S_{10.1}$、$S_{10.5}$

抑制 SYN 泛洪攻击管制器。

- 目的 IP 地址＝IP *A* 或 IP *B*。
- IP 首部协议字段值＝6(TCP)。
- TCP 首部控制标志位：SYN＝1，ACK＝0。
- 速率限制：平均传输速率＝64Kb/s，突发性数据长度＝8000B。

抑制 DDOS 管制器。

- 目的 IP 地址＝IP *A* 或 IP *B*。
- IP 首部协议字段值＝1(ICMP)。
- ICMP 类型字段值：8(ECHO 请求)或 0(ECHO 响应)。
- 速率限制：平均传输速率＝64Kb/s，突发性数据长度＝8000B。

管制器中实际配置的传输速率和突发性数据长度必须考虑正常应用下的最大需求，否则会降低正常应用时的服务性能。

4.5　网络地址转换

为了安全，有时需要隐藏某个内部网络，因此，实际应用中经常见到图 4.31 所示的网络结构，某个内部网络通过边缘路由器接入 Internet，内部网络中的终端分配本地 IP 地

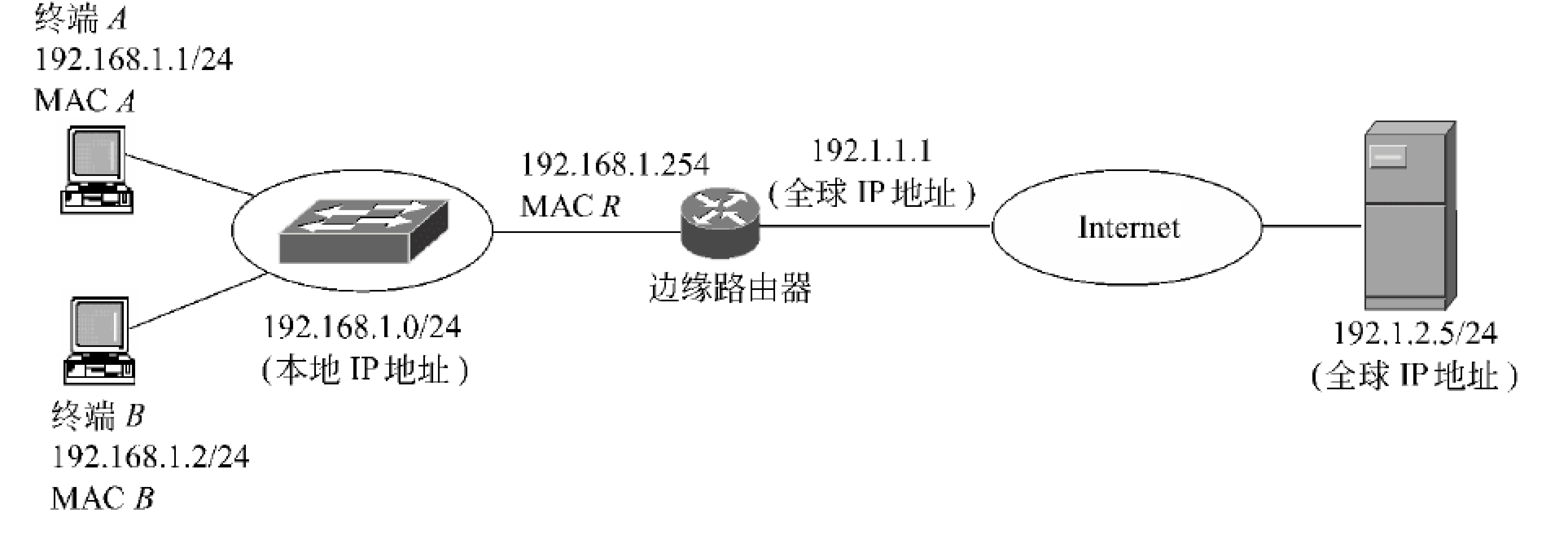


图 4.31　本地 IP 地址和全球 IP 地址共存的情况

址,但本地 IP 地址只在内部网络有效,内部网络中终端发送的、以发送终端本地 IP 地址为源 IP 地址的 IP 分组一旦通过边缘路由器进入 Internet,源和目的 IP 地址都必须转换成全球 IP 地址;否则,无法经过 Internet 实现相互通信。因此,边缘路由器必须具有全球 IP 地址和本地 IP 地址之间的转换功能,这种转换就是网络地址转换(Network Address Translation,NAT)。分配给内部网络的本地 IP 地址和全球 IP 地址之间不应重叠,否则有可能出现内部网络终端希望通信的某个外部网络终端的全球 IP 地址恰巧和内部网络中的某个终端的本地 IP 地址相同的情况,导致内部网络终端发送的、以该外部网络终端的全球 IP 地址为目的 IP 地址的 IP 分组被错误地传输给内部网络中的终端。因此,IETF 推荐三组不在全球 IP 地址范围内的 IP 地址作为内部网络的本地 IP 地址。三组 IP 地址是:

(1) 10.0.0.0/8;

(2) 172.16.0.0/12;

(3) 192.168.0.0/16。

4.5.1 端口地址转换

当图 4.32 中分配了本地 IP 地址的终端想访问 Internet 中的服务器(192.1.2.5)时,就构建一个以本地 IP 地址(192.168.1.1)为源 IP 地址,服务器 IP 地址(192.1.2.5)为目的 IP 地址的 IP 分组。由于配置终端时,默认网关地址为 192.168.1.254,终端将这样的 IP 分组发送给边缘路由器。分配给终端的本地 IP 地址只在内部网络内有效,Internet 并不认可这种地址分配,如果服务器以此地址作为目的 IP 地址向内部网络内终端发送 IP 分组的话,Internet 是无法正确地将该 IP 分组转发给内部网络内终端的,因此,须用 ISP 分配给边缘路由器的全球 IP 地址作为 IP 分组的源 IP 地址。但由于 ISP 分配给边缘路由器的全球 IP 地址只有一个,如果同时有多个内部网络内的终端访问 Internet 的话,这

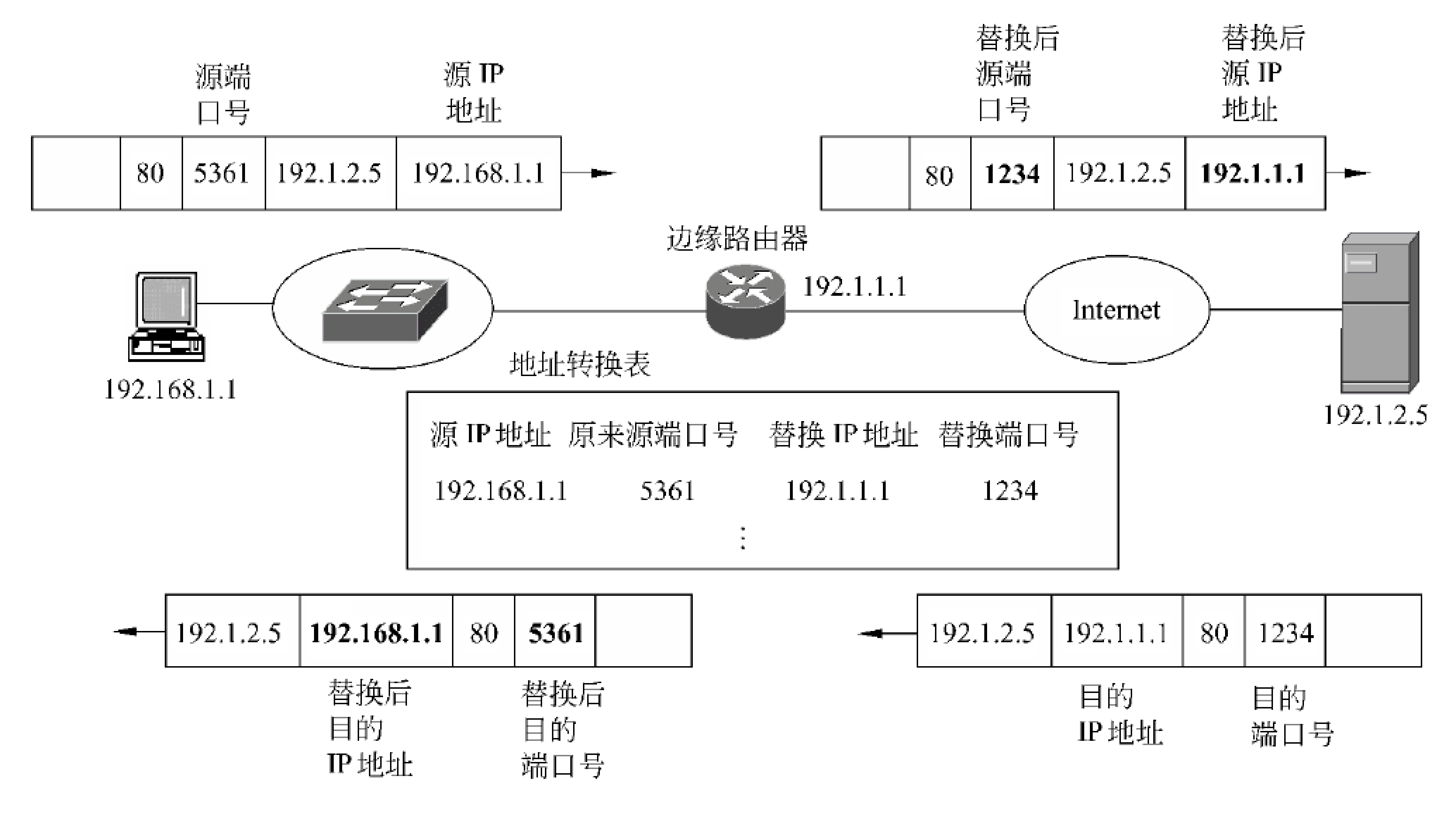


图 4.32 端口地址转换方法实现地址转换的过程

些内部网络内的终端用于访问 Internet 的 IP 分组经过边缘路由器转发后，就有了相同的源 IP 地址(192.1.1.1)，而服务器回复给这些内部网络内的终端的 IP 分组的目的 IP 地址都是相同的，边缘路由器如何能够从这些目的 IP 地址都相同的 IP 分组中鉴别出属于不同内部网络内终端的 IP 分组呢？IP 地址是网络层地址，只能唯一标识网络终端，而通信是进程间的事情，对于多任务系统，终端上可能同时运行多个进程，因此，必须在运输层报文首部提供用于唯一标识进程的端口号。这样，标识 IP 分组发送实体的信息由两部分组成：源 IP 地址和源端口号，在无法用源 IP 地址唯一标识源终端的情况下，可用源端口号来唯一标识源终端。但源终端运输层进程构建运输层报文时，只是用源端口号唯一标识终端内的发送进程，源端口号具有本地意义，即不同的终端可能用相同的源端口号标识终端内的进程。因此，边缘路由器必须用内部网络内唯一的源端口号取代 IP 分组中原来的源端口号，以此实现用源端口号唯一标识内部网络内终端的目的。这种通过将内部网络内不同终端映射到不同源端口号的方法就是端口地址转换(Port Address Translation，PAT)。边缘路由器在用 ISP 分配给它的全球 IP 地址取代 IP 分组中的源 IP 地址时，必须用内部网络内唯一的源端口号取代 IP 分组中原来的源端口号，然后在地址转换表中记录一项，把 IP 分组原来的源端口号、源 IP 地址和边缘路由器取代的唯一的源端口号和全球 IP 地址绑定在一起。当服务器回送的 IP 分组到达边缘路由器时，用该 IP 分组的目的端口号去检索地址转换表，找到对应项，用对应项中的源 IP 地址、原来的源端口号取代该 IP 分组的目的 IP 地址、目的端口号，然后将取代后的 IP 分组转发给局域网，如图 4.32 所示。

两个进程间的通信过程称为会话，在会话期间，必须采用相同的地址转换过程，即属于同一会话的 IP 分组，转换后的源 IP 地址和源端口号必须相同，因此，必须将图 4.33 中的地址转换表中的每一项和某个会话绑定在一起，在该会话开始时创建该转换项，在会话结束时删除该转换项。每一个会话用源和目的 IP 地址、源和目的端口号唯一标识。

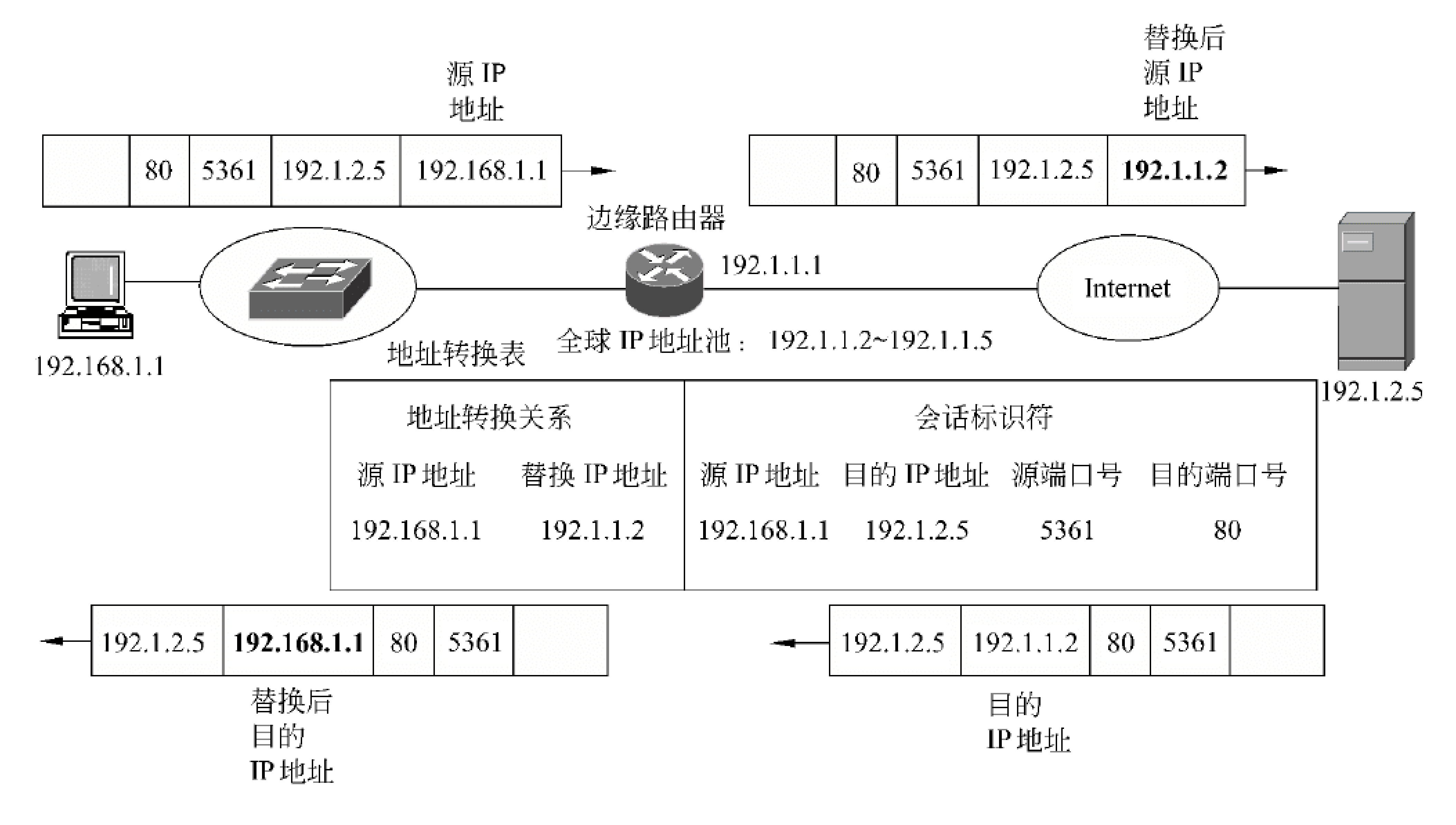


图 4.33　动态 NAT 方法实现地址转换的过程

4.5.2 动态 NAT

动态 NAT 和端口地址转换不同，它分配给内部网络一组，而不是一个全球 IP 地址，所有希望访问 Internet 的终端先申请一个全球 IP 地址，如果分配给内部网络的全球 IP 地址没有分配完，路由器就分配一个全球 IP 地址给该终端，在会话存在期间，该全球 IP 地址一直被该终端使用。一旦会话结束，路由器收回分配该终端的全球 IP 地址。

假定为图 4.33 中的内部网络分配了一组全球 IP 地址(192.1.1.2～192.1.1.5)，当本地 IP 地址为 192.168.1.1 的内部终端发送和 Internet 中某个终端的会话的第一个 IP 分组时，路由器从还没有分配的全球 IP 地址中选择一个全球 IP 地址(192.1.1.2)分配该终端，并将地址转换关系和终端开始的会话绑定在一起，参见图 4.33 中的转换表。以后，所有由本地 IP 地址为 192.168.1.1 的终端发送的、属于该会话的 IP 分组，源 IP 地址一律用 192.1.1.2 替代。同样，路由器一旦接收到的来自 Internet 目的 IP 地址为 192.1.1.2的 IP 分组，将目的 IP 地址还原为 192.168.1.1。如果内部终端发送和 Internet 中某个终端的会话的第一个 IP 分组时，路由器已经分配完所有全球 IP 地址，路由器将丢弃该 IP 分组，使其无法开始和 Internet 中某个终端的会话。从原理上讲，动态 NAT 可用于净荷不是运输层报文的 IP 分组，但由于地址映射是针对会话，而不是单个 IP 分组的，因此，必须具有明确的开始和结束标志的通信过程才能使用动态 NAT。

4.5.3 静态 NAT

无论是端口地址转换还是动态 NAT 都只能实现单向会话，即会话发起者必须是内部网络中的终端，由内部网络中的终端发送和 Internet 中某个终端的会话的第一个 IP 分组，由该 IP 分组在内部网络和外部网络之间的边缘路由器建立地址转换关系及地址转换关系和相关会话的绑定。如果 Internet 中的终端希望发起和内部网络中的终端的会话，由于在边缘路由器建立内部网络中的终端的本地 IP 地址和某个全球 IP 地址之间的地址转换关系前，无法获得内部网络中的终端的全球 IP 地址，因而无法向内部网络中的终端发送 IP 分组。因此，如果想要实现双向会话，无须内部网络中的某个终端发送和 Internet 中的终端的会话的第一个 IP 分组，就在边缘路由器建立该终端的本地 IP 地址和某个全球 IP 地址之间的映射，这种地址转换方法就是静态 NAT，它通过配置，在边缘路由器建立某个内部网络终端的本地 IP 地址和全球 IP 地址之间的映射，这样，外部网络终端就可用该全球 IP 地址发起和该内部网络终端的会话，整个过程如图 4.34 所示。

4.5.4 NAT 的弱安全性

除了静态 NAT 外，在内部网络中的终端发起某个会话前，外部网络中的终端是无法访问到内部网络中的终端的，因此，也无法发起对内部网络中的终端的攻击，这是 NAT 被作为网络安全机制的主要原因，但一旦内部网络中的某个终端发起访问外部网络中的终端的会话，而且黑客终端截获到内部网络中的终端发送的、经过边缘路由器 NAT 后的 IP 分组，黑客终端就可以通过该 IP 分组给出的源端口号和源 IP 地址对内部网络中的终端实施攻击，因此，NAT 更多是被作为解决 IP 地址短缺问题的方法，解决内部网络的安

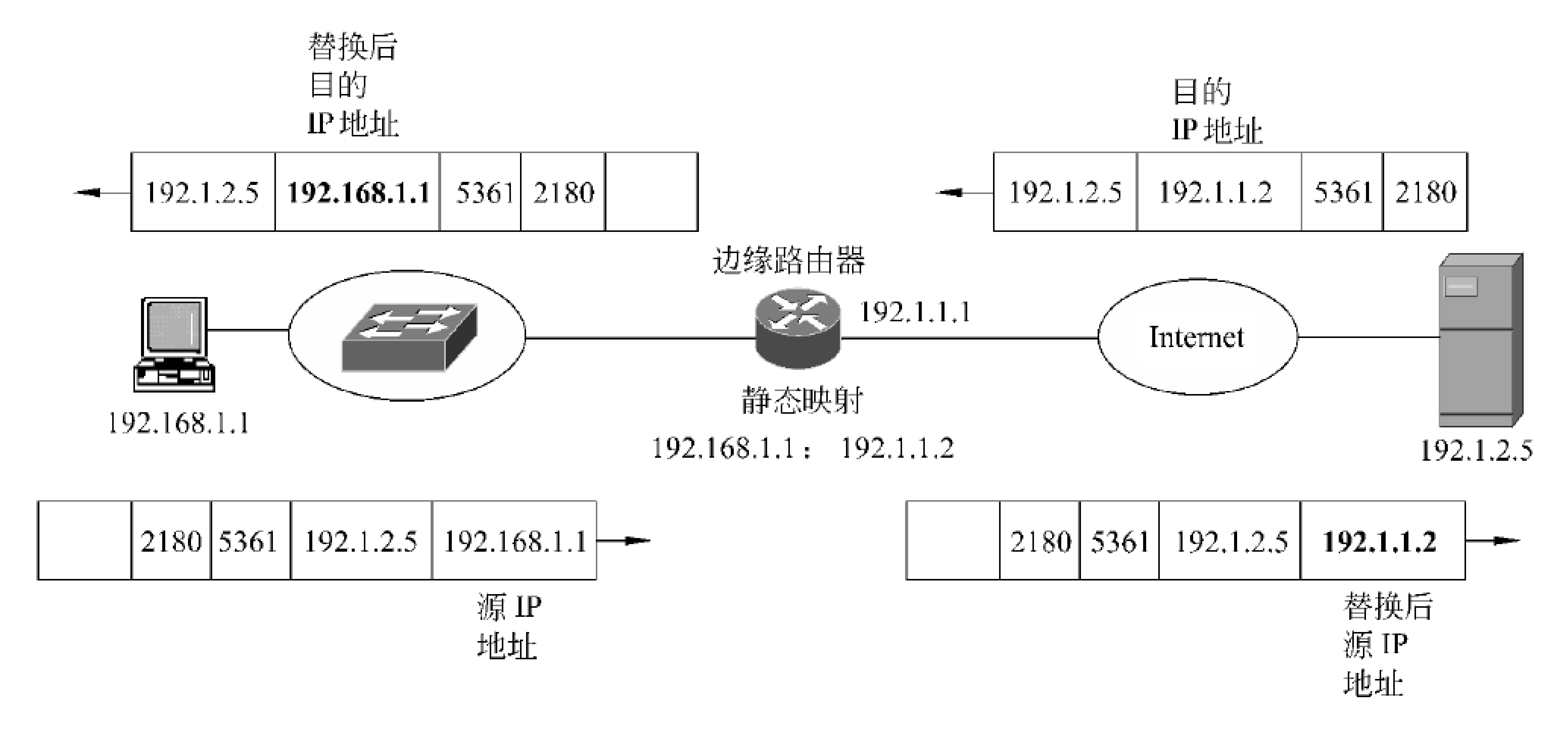


图 4.34　静态 NAT 方法实现地址转换的过程

全问题需要用防火墙技术，仅仅用 NAT 是不够的，NAT 的弱安全性只能是其他网络安全技术的一种补充。

4.6　容错网络结构

计算机网络安全的主要目标是保证网络的适用性，这就要求安全网络在若干网络结点或链路失效的情况下仍能保证网络的连通性，容错网络结构就是一种满足上述安全特性的安全网络结构。

4.6.1　核心层容错结构

图 4.35 所示的网络结构是一种常见的局域网或城域网结构，核心层由高速交换机组成，实现各个子网间 IP 分组的线速转发，汇聚层由路由器（也可以是三层交换机）组成，主

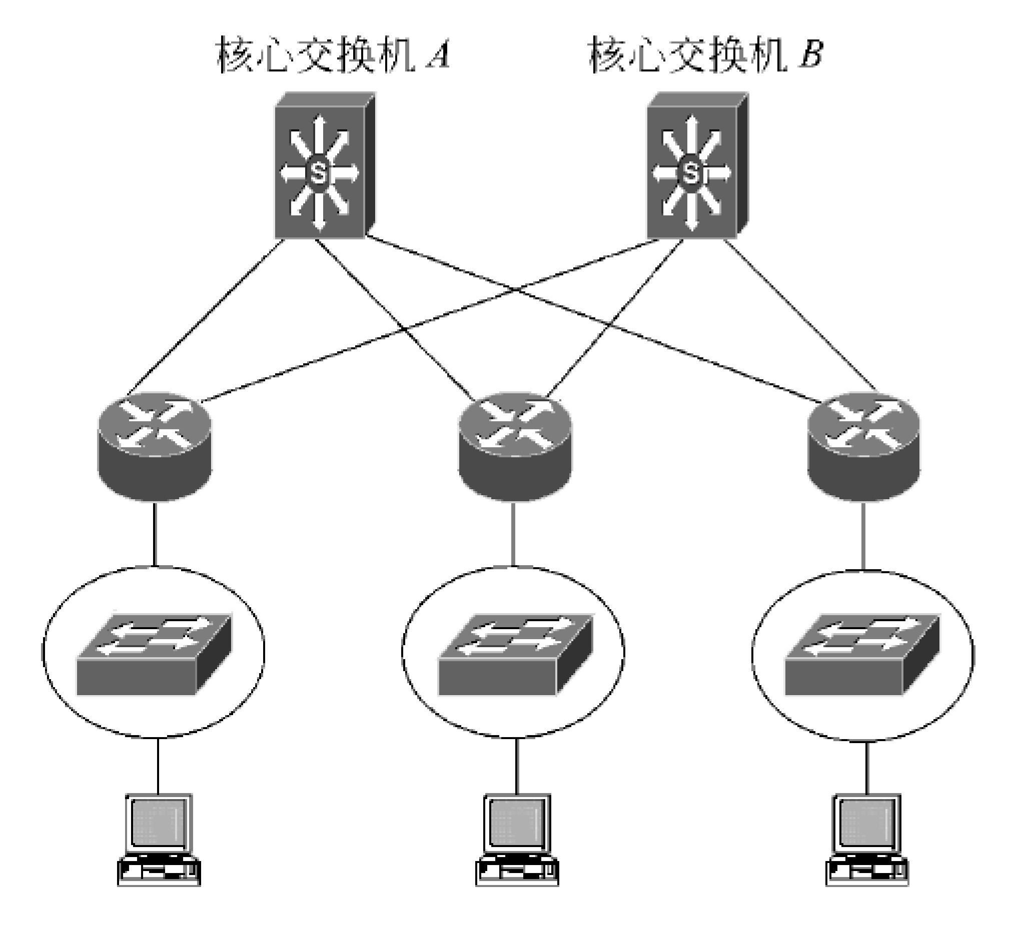


图 4.35　核心层容错结构

要完成信息流的管理和控制功能，如报文过滤、流量管制等。这种网络结构，核心层是整个网络的中枢，一旦核心层交换机出错，整个网络将瘫痪，因此，核心层交换机必须采取冗余结构，如图 4.35 所示的双核心层交换机结构，而且，对于安全性要求较高的网络系统，双核心层交换机必须异地设置，避免火灾、断电这样的事故使双核心层交换机同时失效。

4.6.2 网状容错结构

网状拓扑结构导致路由器之间存在多条传输路径，路由协议动态生成传输路径的机制保证在某个路由器或某条链路失效的情况下，仍然能够产生新的端到端传输路径，如图 4.36所示，正常情况下，终端 A 至终端 B 的传输路径是终端 A→路由器 R_1→路由器 R_3→终端 B，一旦路由器 R_1 和 R_3 之间链路失效，各个路由器通过交换路由消息，生成新的传输路径：终端 A→路由器 R_1→路由器 R_4→路由器 R_3→终端 B，保证了两个终端之间的端到端连通性。

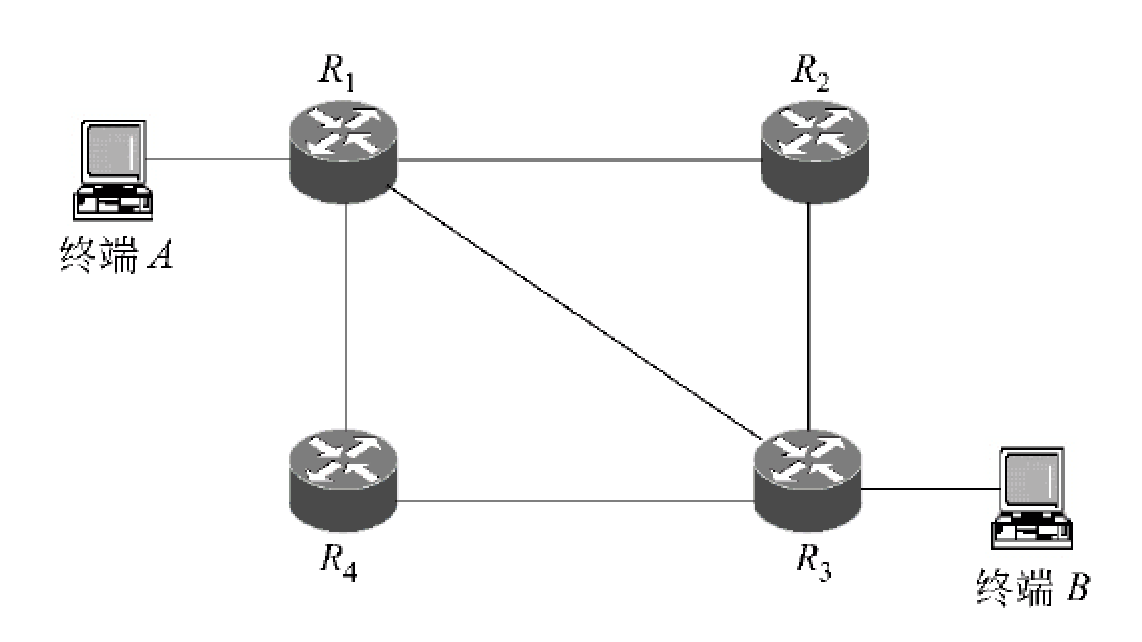


图 4.36 网状容错结构

4.6.3 生成树协议

以太网交换机的转发机制要求交换机之间不允许存在环路，因此，在以太网中，任何两个终端之间只允许存在一条传输路径，但这种网络结构的可靠性不高，任何一段链路发生故障，就有可能使一部分终端无法和网络中的其他终端通信。是否能够设计这样一种网络，它存在冗余链路，但在网络运行时，通过阻塞某些端口使整个网络没有环路，当某条链路因为故障无法通信时，通过重新开通原来阻塞的一些端口，使网络终端之间依然保持连通性，而又没有形成环路，这样，既提高了网络的可靠性，又消除了环路带来的问题。生成树协议(Spanning Tree Protocol，STP)就是这样一种机制，图 4.37 就是描述生成树协议作用过程的示意图。

图 4.37(a)是原始网络拓扑结构，交换机之间存在环路，通过运行生成树协议，生成图 4.37(b)所示的既保持交换机之间连通性，又避免环路问题的网络拓扑结构，这种以太网结构能够保证 MAC 帧的正常转发，如图 4.37(b)所示。如果以太网结构由于交换机之间链路故障，导致交换机之间连通性被破坏，如图 4.37(c)所示。生成树协议通过重新启用被阻塞的冗余链路，再次保证新的以太网结构中交换机之间的连通性，如图 4.37(d)所示。

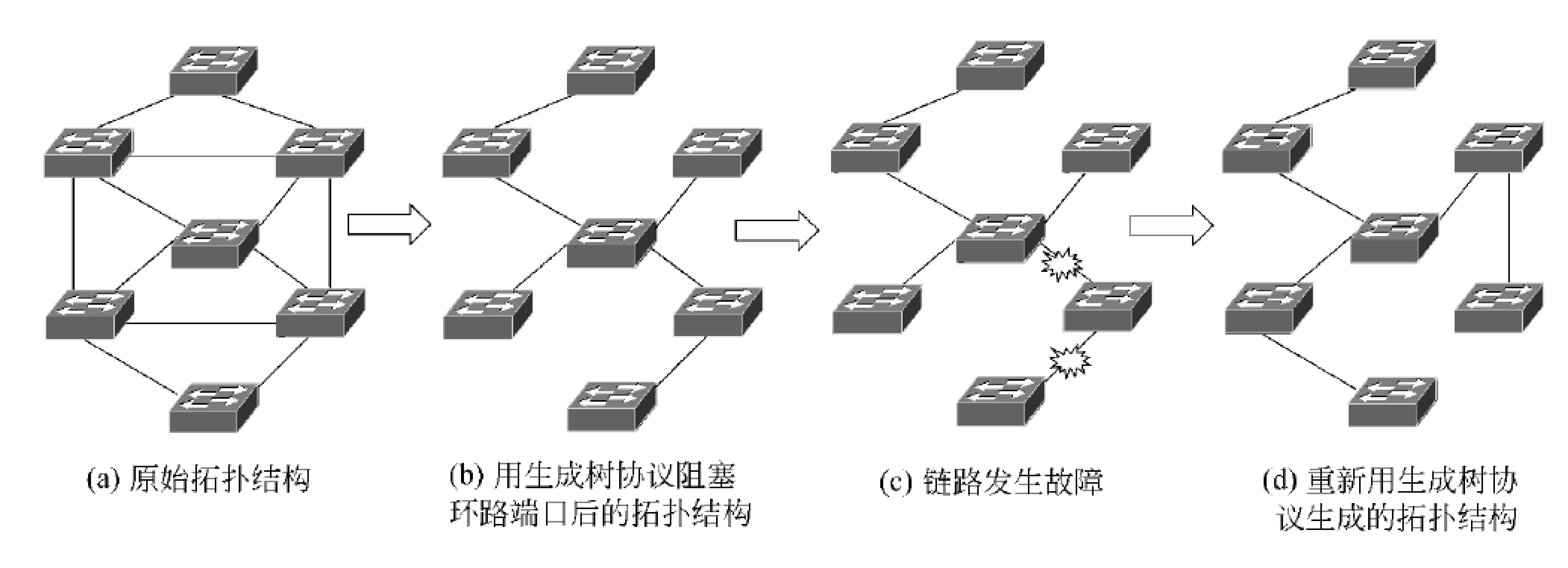


图 4.37　生成树协议容错机制

4.6.4　冗余链路

生成树协议能够解决以太网的容错问题，但一是以太网运行生成树协议的开销较大，二是从链路发生故障到通过生成树协议重新构建新的保证交换机之间连通性的以太网结构的时间较长，在这段时间内，可能因为故障链路导致以太网不能正常转发 MAC 帧。关键链路实施容错可以采用图 4.38 所示的冗余链路技术，交换机 *C* 同时和交换机 *A* 和交换机 *B* 相连，连接交换机 *A* 的链路为主链路，处于正常传输状态，连接交换机 *B* 的链路为备用链路，在主链路处于正常传输状态时，交换机 *C* 连接备用链路的端口处于阻塞状态，因此，图 4.38 所示的网络结构等同于图 4.39(a)所示的以太网结构，交换机之间保证连通，且没有环路。一旦主链路发生故障，交换机 *C* 通过监测物理层信号检测到故障，立即阻塞连接主链路的端口，启用连接备用链路的端口，备用链路处于正常传输状态，如图 4.39(b)所示，以太网依然保持连通性且没有环路。

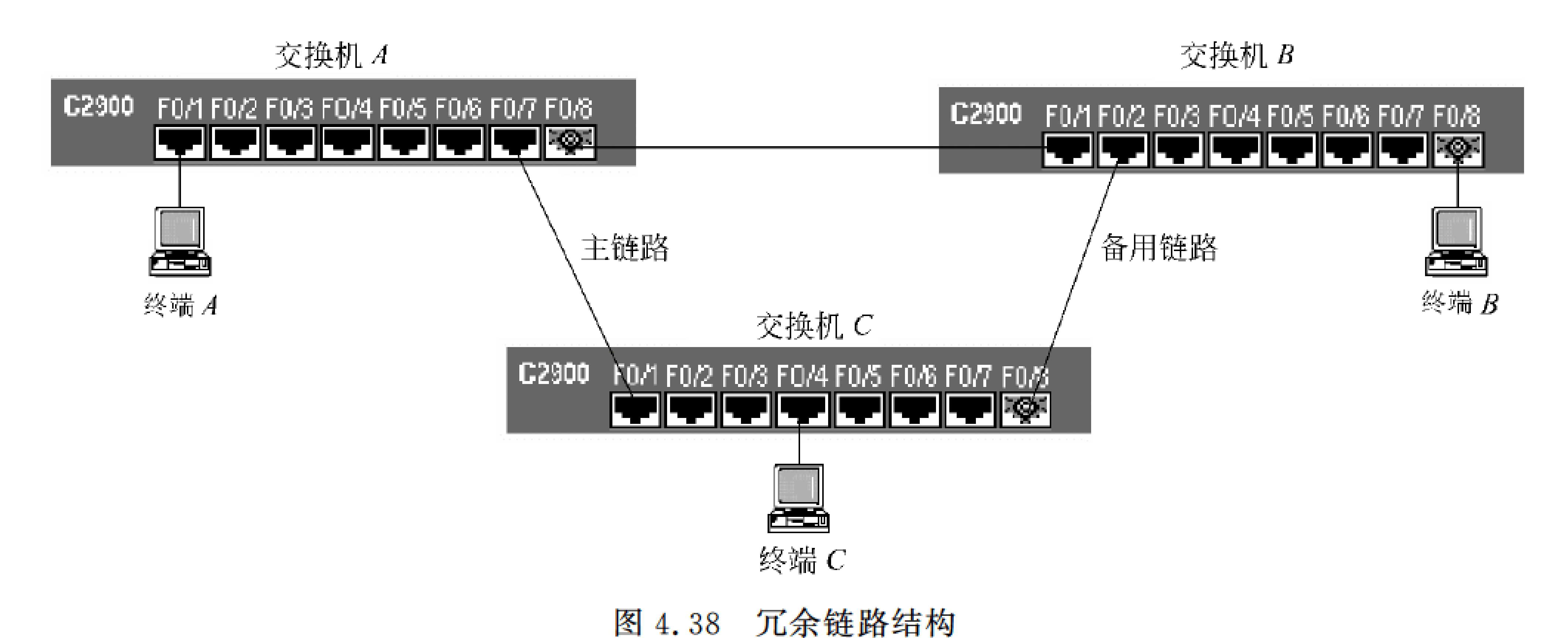


图 4.38　冗余链路结构

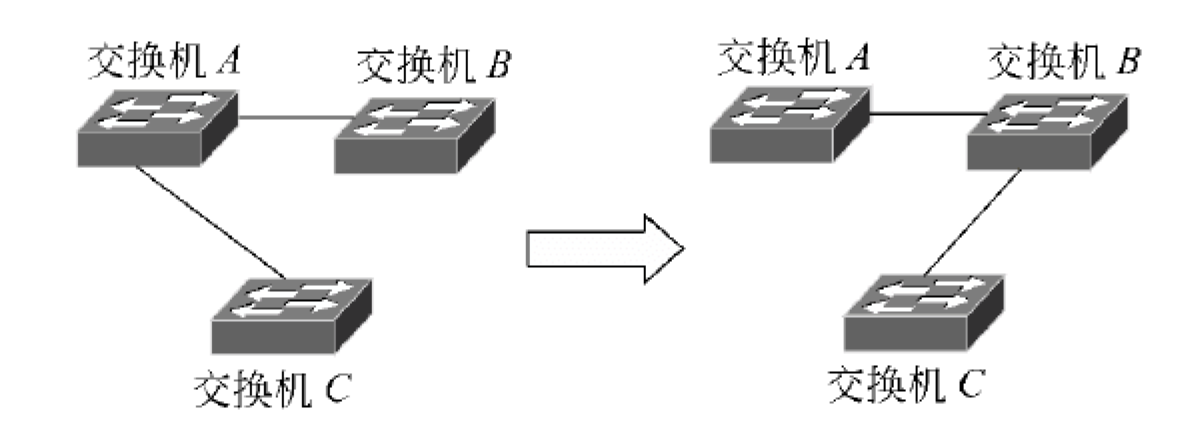


图 4.39 冗余链路容错机制

习 题

4.1 以太网有哪些接入控制技术？采用接入控制对网络安全有什么影响？

4.2 对于手工配置网络信息的终端，如何避免遭到 ARP 欺骗攻击？

4.3 列出常见的攻击以太网的方法，并提出解决方案。

4.4 针对图 4.40 所示的网络结构，给出用 802.1X 实现接入终端认证所需要的配置。

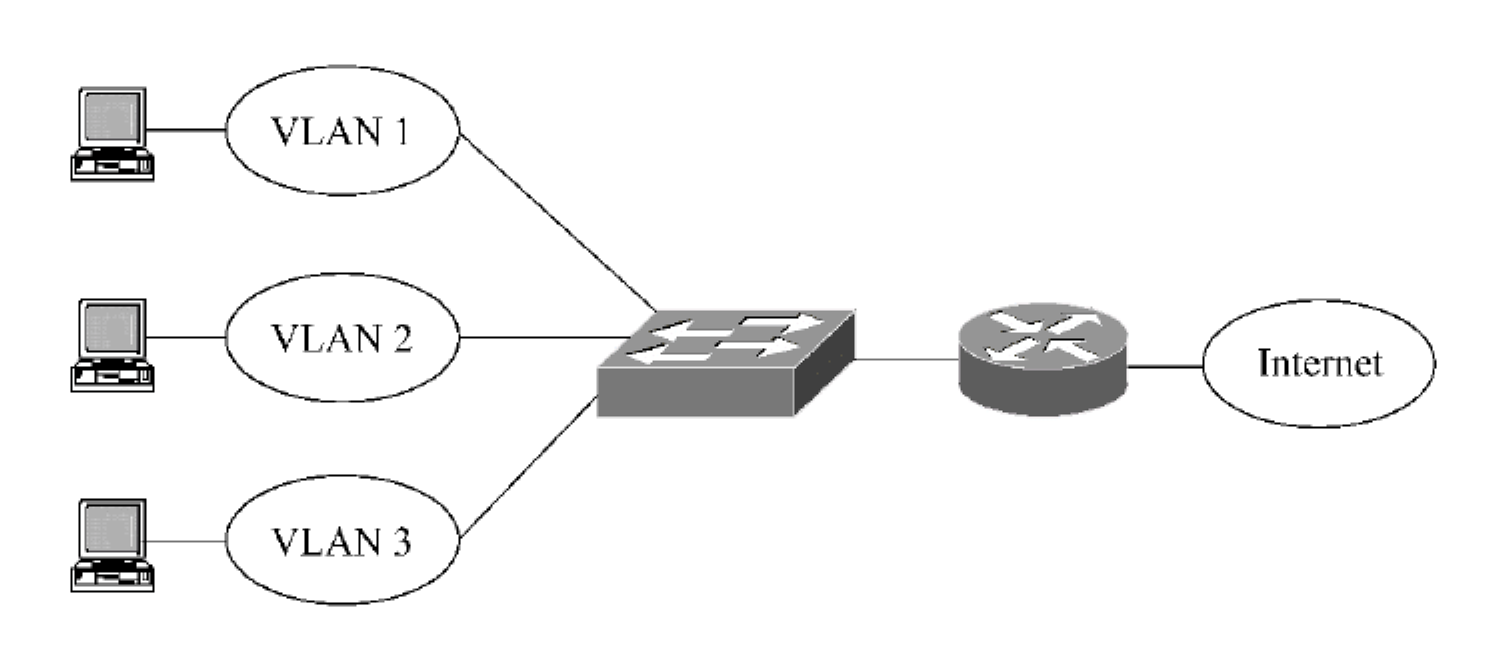


图 4.40 题 4.4 图

4.5 路由器之间如何认证相互交换的路由消息？

4.6 路由器如何防止源 IP 地址欺骗攻击？这种防止机制有什么前提？对于非对称路径，即两端两个传输方向所对应的传输路径不同，这种防止机制会造成什么后果？

4.7 根据虚拟技术将图 4.41 所示网络分成两个独立的网络，其中网络 1 包含终端 *A*、*C*、*E* 和 FTP 服务器，网络 2 包含终端 *B*、*D*、*F* 和 Web 服务器，对于网络 1 要求终端 *A*、*C* 属于一个 VLAN，终端 *E* 单独属于一个 VLAN，FTP 服务器单独属于一个 VLAN。对于网络 2 要求终端 *B*、*D* 属于一个 VLAN，终端 F 单独属于一个 VLAN，Web 服务器单独属于一个 VLAN。请给出交换机和路由器配置。

4.8 假定图 4.41 是一个完整的内部网络结构，如何限制终端访问服务器的速率，假定 FTP 和 Web 服务器的平均访问速率限制为 50Mb/s，如何通过限制终端访问服务器速率，保证所有终端访问服务器的平均速率之和不超过 50Mb/s？如何确定每一个终端的突发性数据长度？

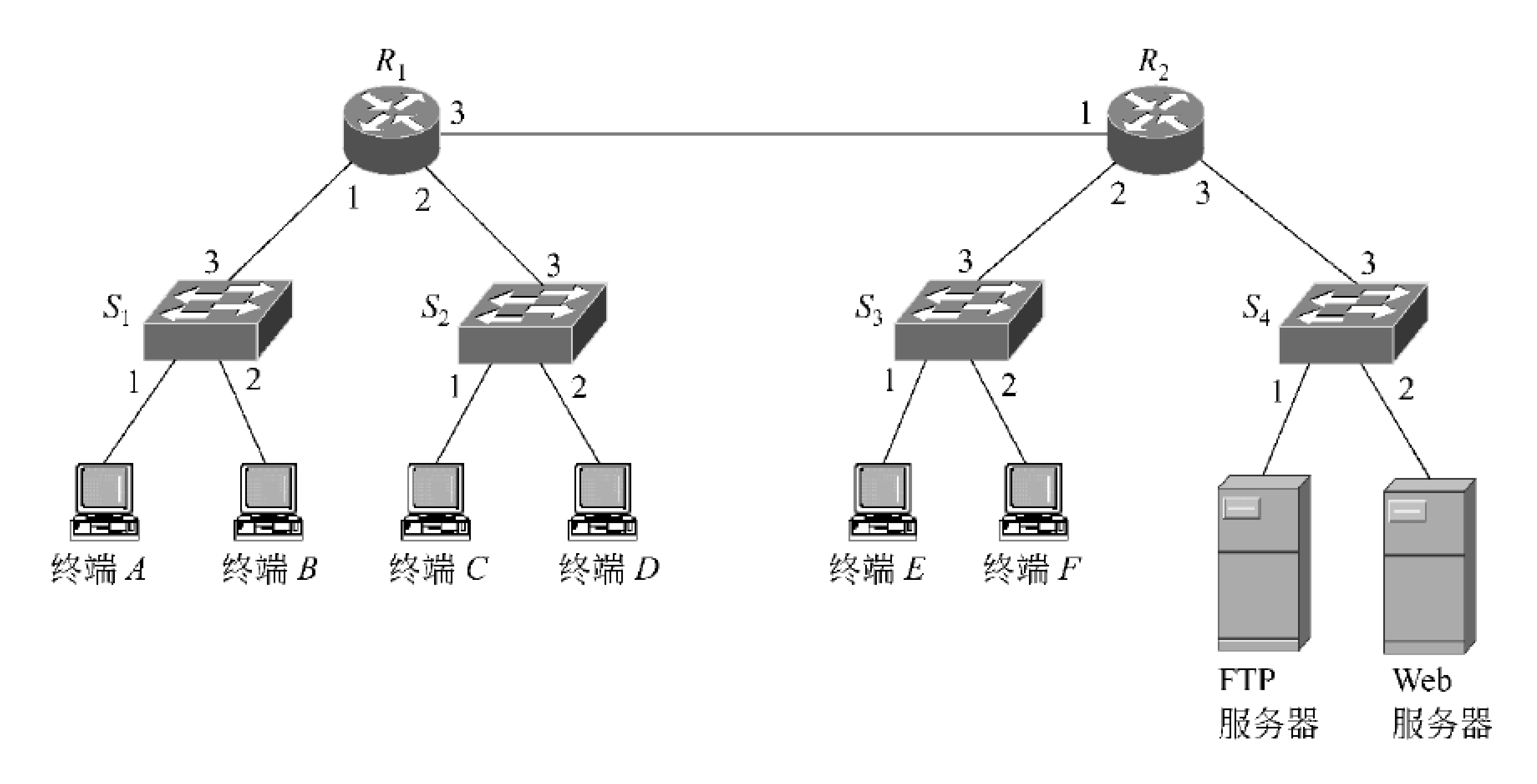


图 4.41　题 4.7 图

4.9　本地局域网通过 ADSL 路由器接入 Internet 的结构如图 4.42 所示，请给出本地 IP 地址为 192.168.1.1 的终端访问 Internet 中服务器的过程。

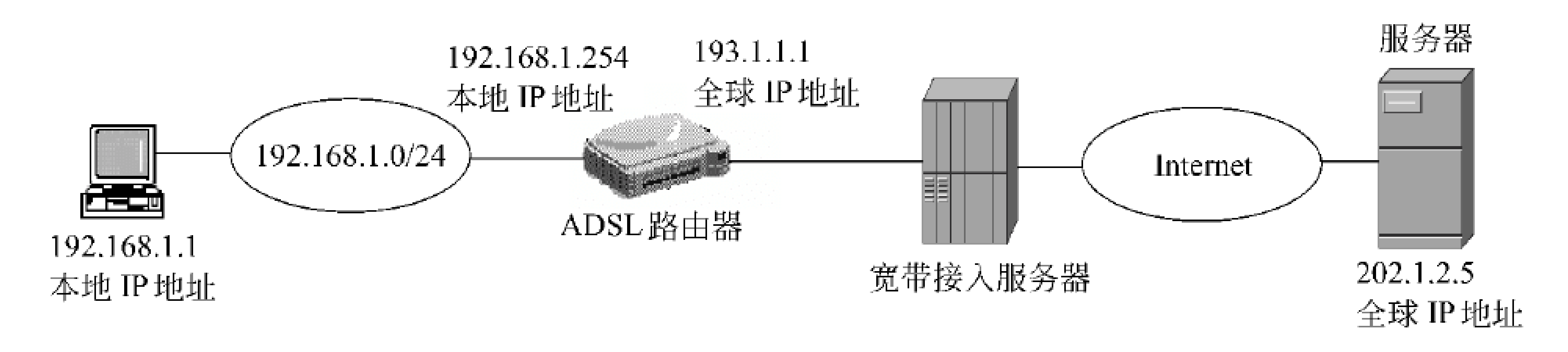


图 4.42　题 4.9 图

4.10　NAT 的安全性如何体现？

4.11　请给出 NAT 解决 IPv4 地址短缺问题的思路。

4.12　为什么说网状结构的分组交换网络比 PSTN 的容错性要好？

4.13　实现以太网容错功能的技术有哪些？

第 5 章 无线局域网安全技术

CHAPTER

无线局域网(Wireless LAN,WLAN)是一种利用无线电波在自由空间的传播实现终端之间通信的网络,用无线局域网通信的最大好处是终端之间不需要铺设线缆,这一特性不仅使无线局域网非常适用于中间隔着湖泊、公共道路等不便铺设线缆的网络应用环境,而且,解决了网络终端的移动通信问题。由于这几年笔记本计算机已经得到普及,人们在工作过程中不时携带笔记本计算机更换工作场合,而且,需要随时利用笔记本计算机访问网络,这就使得移动通信的需求不断增长,导致无线局域网在近几年得到飞速发展。但无线局域网的无线通信方式使得无线局域网的通信安全成为很大的问题,如果发生这样的事情:将一端连接内部以太网交换机端口的双绞线电缆弃置大楼外广场,任何一台终端只要插入该双绞线电缆就能访问内部网络,谁都会觉得不可思议,但如果缺乏安全技术,无线局域网就好像是有无数一端连接内部以太网交换机端口的双绞线电缆弃置大楼外广场的以太网。

5.1 无线局域网的开放性

5.1.1 频段的开放性

无线局域网所使用的频段基本属于 ISM(Industrial,Scientific,and Medical)频段,这些频段称为工业、科学和医疗所使用的电磁波频段,是为了满足公众利用无线电进行通信的需求,允许公众自由使用的开放电磁波频段,图 5.1 是美国开放的电磁波频段,大多数国家都与此兼容。

无线局域网使用的电磁波频段为 2.412～2.462GHz、5.15～5.35GHz 和 5.725～5.825GHz 这三个频段,它们和 ISM 频段基本兼容。利用标准和开放的电磁波频段进行无线通信,意味着任何能够接收这些频段的信号的无线电设备都能截获无线局域网用于数据通信的无线电信号并根据无线局域网的调制原理还原出数据。

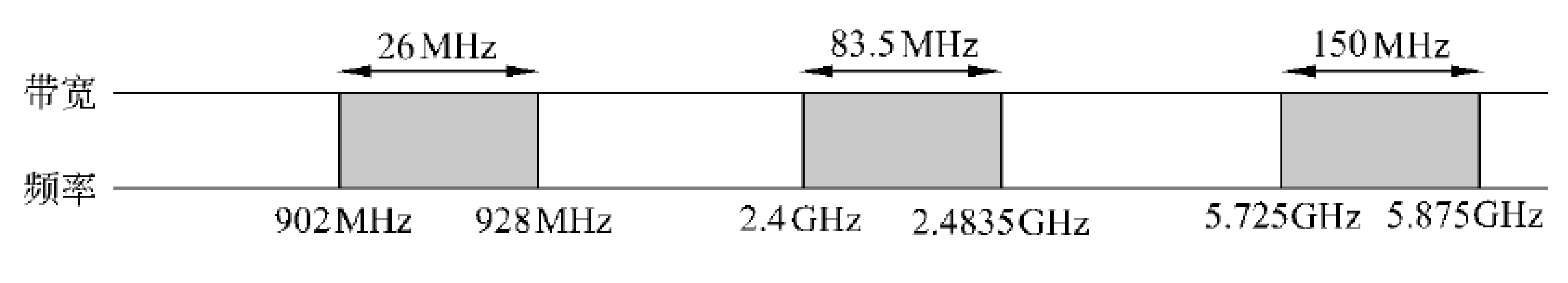


图 5.1 美国开放的电磁波频段

5.1.2 空间的开放性

无线通信方式下，电磁波在自由空间传播，信号的传播范围取决于信号发射时的能量，图 5.2 是某个发射装置所发射的电磁波的传播范围，任何处于信号传播范围内的接收设备都能接收到该发射装置所发射的电磁波信号。

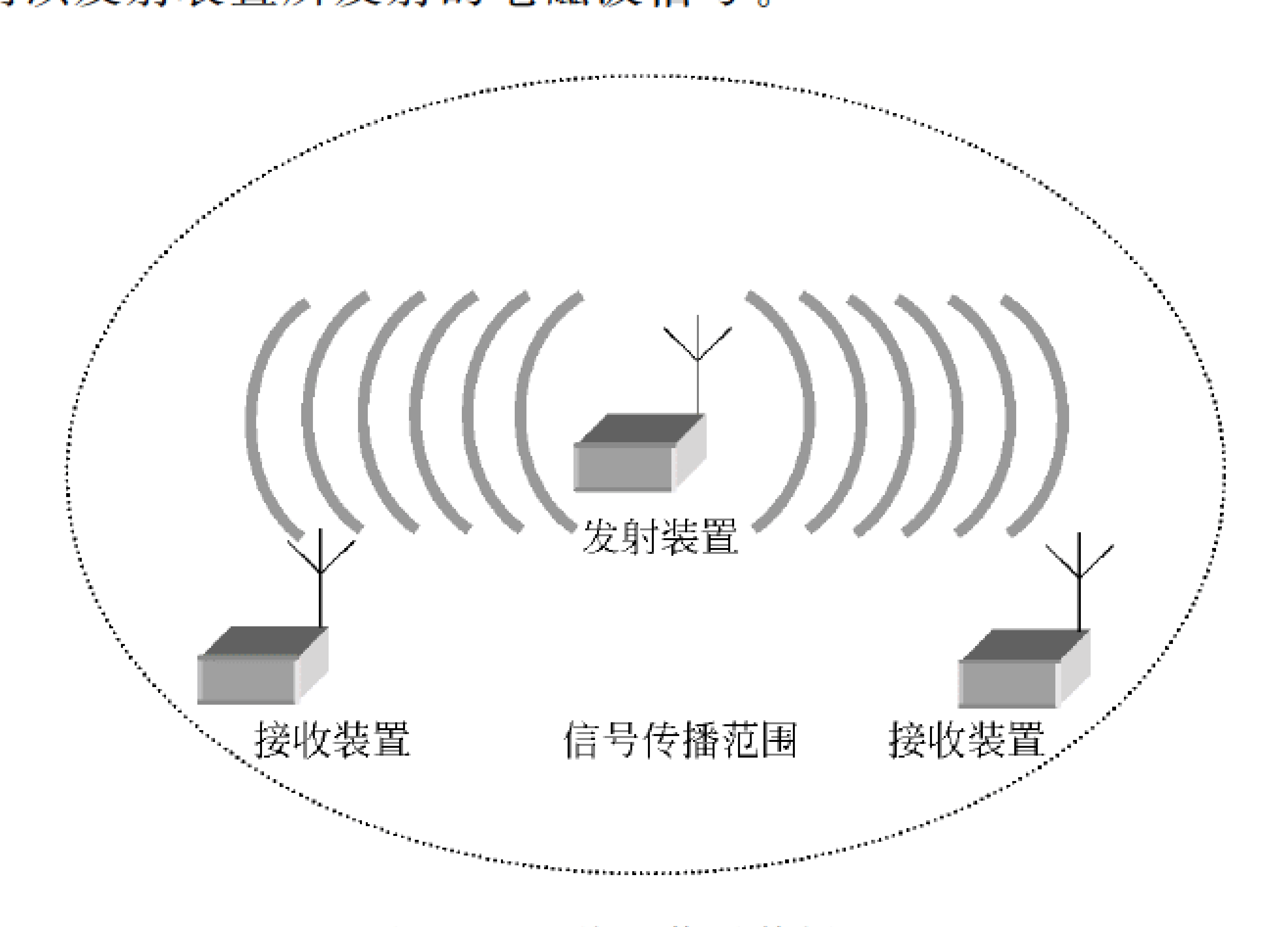


图 5.2 无线电信号传播过程

5.1.3 开放带来的安全问题

开放性带来两个安全问题，一是接入控制，二是数据加密。有线网络，如以太网，存在物理接入过程，某个终端接入以太网时，必须用线缆（通常是双绞线电缆）连接以太网交换机端口和终端，因此，可以通过控制物理连接过程对终端接入以太网过程实施控制，同时，通过认证机制对接入终端的身份进行认证，保证只有授权终端才能通过以太网发送或接收数据。但对于如图 5.3 所示的由接入点（Access Point，AP）组成的基本服务集（Basic Service Sets，BSS），无线局域网电磁波自由传播的特性使得任何处于 AP 发射的电磁波信号传播范围内的终端都能和 AP 进行通信，并通过 AP 接入内部网络。

同样，电磁波自由传播的特性使得 BSS 内的任何一个终端都能接收到其他终端和 AP 之间交换的数据，因此，如果不对通过无线局域网传输的数据进行加密，将无法保证数据的保密性。

解决无线局域网安全问题的方法是认证和加密，认证解决接入控制问题，保证只有授权终端才能和 AP 通信，并通过 AP 接入内部网络。为了在无线局域网中实现认证机制，

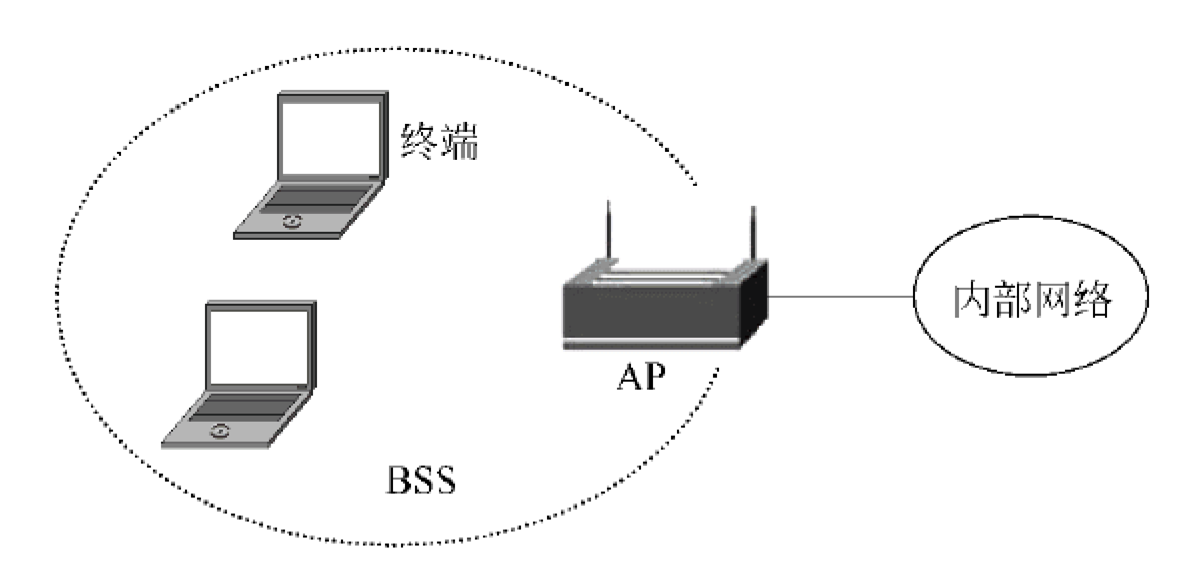


图 5.3　基本服务集

首先必须使终端和 AP 之间有一个类似以太网物理接入过程的虚拟连接建立过程，AP 在建立和终端之间的虚拟连接后，必须对接入终端的身份进行认证，以此保证只有授权终端才能和 AP 进行通信。加密解决终端和 AP 之间传输的数据的保密性问题，对终端和 AP 之间传输的数据进行加密操作，只有拥有密钥的终端才能还原出明文，其他终端即使截获到终端和 AP 之间传输的加密后的数据，也无法得到明文，以此保证数据的保密性。

5.2　WEP 加密和认证机制

5.2.1　WEP 加密机制

802.11 等同有线安全（Wired Equivalent Privacy，WEP）算法加密数据的过程如图 5.4所示。40 位密钥（也可以是 104 位密钥）和 24 位初始向量（IV）串接在一起，构成 64 位随机数种子，伪随机数生成器（PRNG）根据随机数种子产生一次性密钥，一次性密钥的长度为数据长度加上 4 字节的完整性检验值（ICV）。4 字节的完整性检验值是根据数据和生成函数 $G(X)$ 计算所得的循环冗余检验码。一次性密钥和随机数种子是一对一的关系，只要随机数种子改变，一次性密钥也跟着改变。构成随机数种子的 64 位二进制数中，40 位密钥是固定不变的，改变的只能是 24 位的初始向量。为了使接收端能够产生相同的一次性密钥，必须让接收端和发送端同步随机数种子，在 802.11WEP 算法中，发

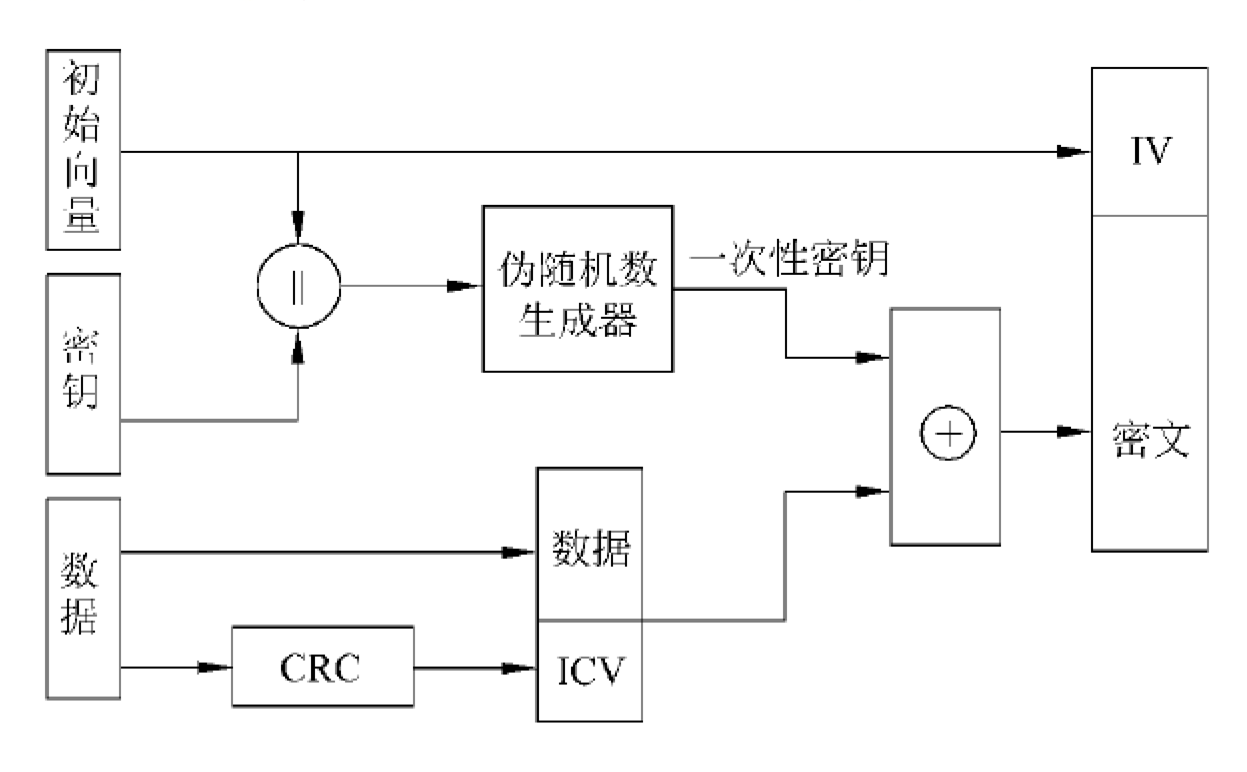


图 5.4　WEP 加密数据过程

送端和接收端具有相同的 40 位密钥,因此,只要同步初始向量,就能同步随机数种子。为此,发送端将 24 位初始向量以明码的方式传输给接收端。数据和 4 字节完整性检验值和相同长度的一次性密钥异或运算后构成密文。为了保证数据传输安全,必须每一次更换一次性密钥,因此,每一次加密数据都须使用不同的初始向量。

解密数据过程如图 5.5 所示,接收端将配置的 40 位密钥和 MAC 帧携带的 24 位初始向量串接成 64 位的随机数种子,伪随机数生成器根据这 64 位随机数种子产生一次性密钥,其长度等于密文长度,密文和一次性密钥异或运算后还原成数据明文和 4 字节的完整性检验值,同样根据数据和生成函数 $G(X)$ 计算出循环冗余检验码,并把计算结果和 MAC 帧携带的完整性检验值比较,如果相等,表示数据在传输过程中没有被篡改。

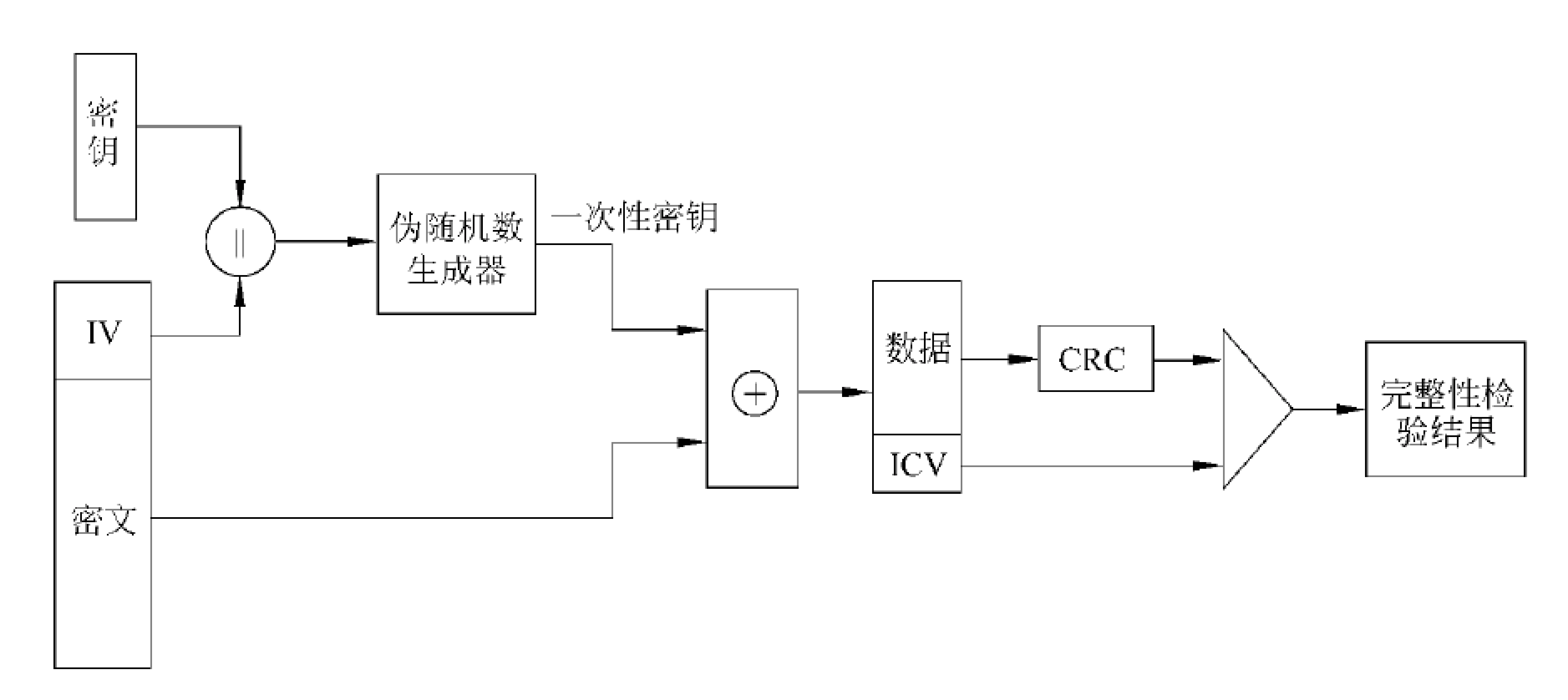


图 5.5 WEP 解密数据过程

5.2.2 WEP 帧结构

经过 WEP 加密运算后的无线局域网帧结构如图 5.6 所示,一旦控制字段中 WEP 位置 1,原来由数据组成的净荷字段扩展成图 5.6 所示的格式,它由明文方式的 24 位 IV,6 位填充位,2 位密钥标识符,若干字节由数据加密后生成的密文,和 4 字节由完整性检验值(Integrity Check Value,ICV)加密后生成的密文组成,填充位固定为 0,2 位密钥标识符允许发送端和接收端在 4 个密钥中选择一个用于当前 MAC 帧加密运算的密钥,ICV 的计算方式与 MAC 帧的帧检验序列(FCS)字段相同,采用如下生成函数计算出循环冗余检验(Cyclic Redundancy Check,CRC)码。

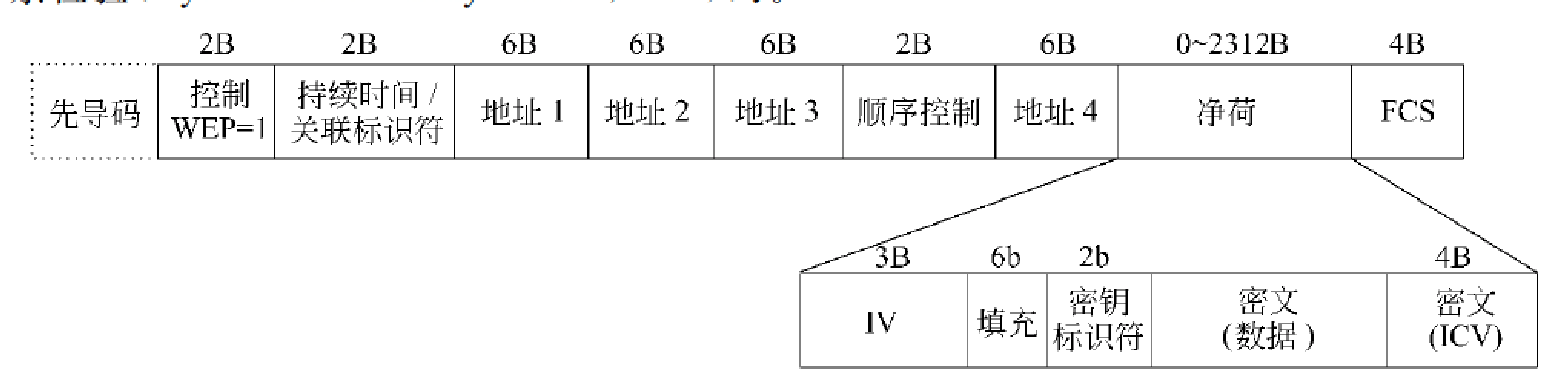


图 5.6 WEP 帧结构

$$G(x)=x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^{8}+x^{7}+x^{5}+x^{4}+x^{2}+x+1$$

但计算FCS字段的CRC码时，数据序列包含MAC帧的各个字段，计算ICV时，数据序列只包含MAC帧的数据字段。FCS用于检测MAC帧传输过程中发生的错误，人为地篡改是无法检测的，因为篡改者在篡改MAC帧后，可以重新计算FCS字段值。由于经过无线局域网传输的是对ICV加密运算后生成的密文，因此，篡改者无法先对数据密文进行篡改，然后根据篡改后的数据密文重新计算ICV，并对重新计算后的ICV进行加密，因此，ICV可用于检测数据密文传输过程中是否被篡改。第3章中常用报文摘要来进行数据完整性检测，和根据MD5或SHA-1报文摘要算法生成的报文摘要相比，CRC码的完整性检测功能要弱得多。

5.2.3 WEP认证机制

802.11WEB算法定义了两种认证机制，一是开放系统认证机制，二是共享密钥认证机制，开放系统认证机制实际上并不对终端进行认证，只要终端向AP发送认证请求帧，AP一定向终端回送表示认证成功的认证响应帧。共享密钥认证过程如图5.7所示，终端向AP发送认证请求帧，AP向终端回送认证响应帧，认证响应帧中包含由AP伪随机数生成器产生的长度为128字节的随机数challenge，终端接收到AP以明文方式表示的随机数challenge后，按照图5.4所示的WEP加密数据过程对随机数challenge进行加密，以密文和初始向量为净荷构建认证请求帧，并把认证请求帧发送给AP。AP根据图5.5所示的WEP解密数据过程还原出随机数challenge，并将还原出的随机数challenge和自己保留的随机数challenge比较，如果相同，表示认证成功，向终端发送表示认证成功的认证响应帧。否则，表示认证失败，向终端发送表示认证失败的认证响应帧。图5.7中发送的认证请求和响应帧都携带认证事务序号，从终端发送的第一个认证请求帧开始，认证事务序号依次为1～4，因此，终端发送给AP的两个认证请求帧由于认证事务序号分别为1和3，AP对其进行的操作也不同。共享密钥认证机制确定某个终端是否是授权终端的依据是该终端是否具有AP所具有的密钥。

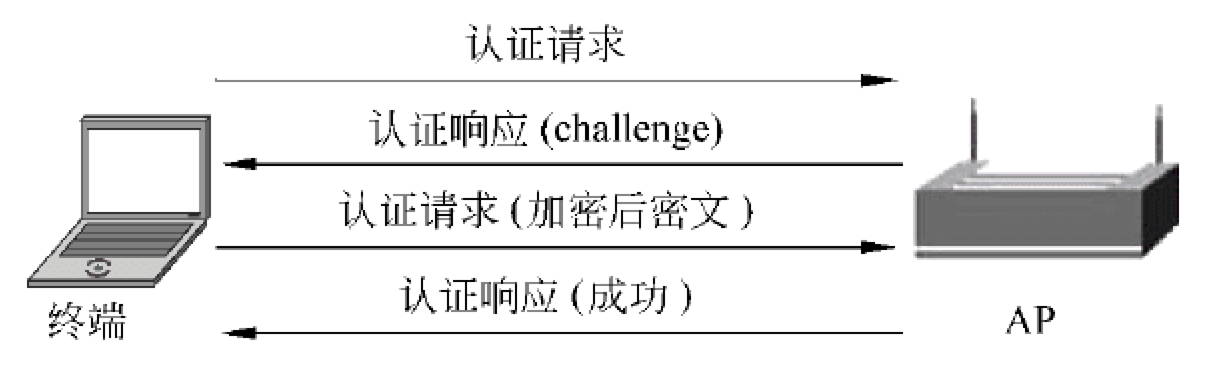


图5.7　共享密钥认证过程

5.2.4 基于MAC地址认证机制

基于MAC地址认证机制并不是WEP要求的认证机制，但目前许多生产厂家生产的AP都支持这一认证机制，AP建立授权终端的MAC地址列表，某个终端接入AP前，先向AP发送认证请求帧，认证请求帧中须指明认证机制：MAC地址认证，AP用该MAC帧的源地址去检索授权终端的MAC地址列表，如果找到匹配地址，发送认证成功的认证

响应帧，否则，发送认证失败的认证响应帧，认证过程如图 5.8 所示。

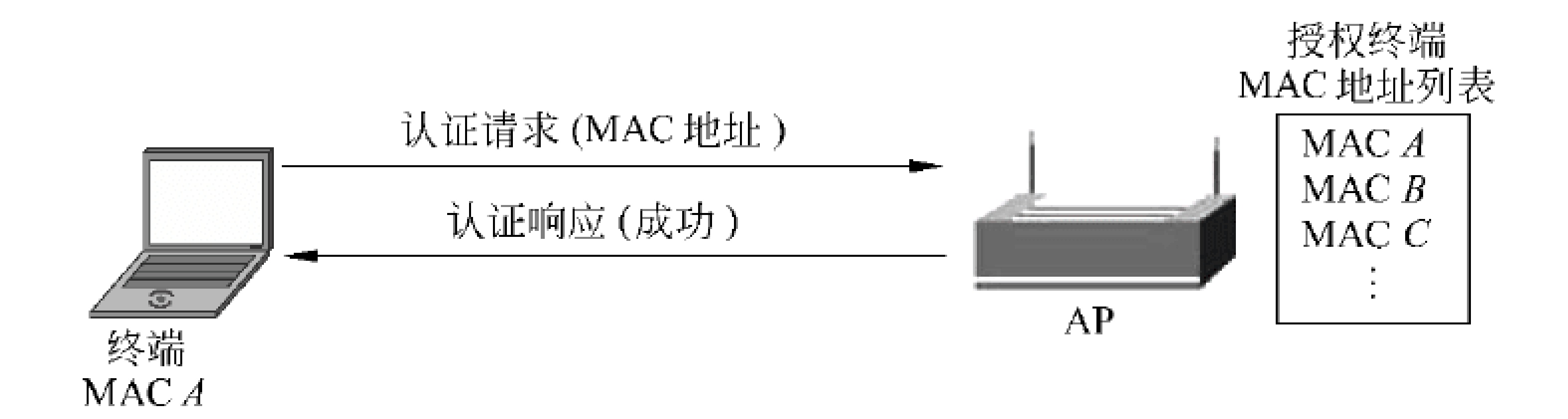


图 5.8 基于 MAC 地址认证过程

早期无线局域网卡和以太网卡上都有固化的 MAC 地址，该 MAC 地址不但是全球唯一的，而且是无法改变的，因此，用 MAC 地址标识终端是有效的，由于目前的驱动程序并不一定用网卡上固化的 MAC 地址作为该终端发送的 MAC 帧的源地址，而是可以用某个逻辑 MAC 地址替换网卡上固化的物理 MAC 地址，因此，用 MAC 地址标识终端的方式已不再可靠，越来越多的攻击采用源 MAC 地址欺骗方式。

5.2.5 关联的接入控制功能

终端和 AP 进行数据交换前，必须先和 AP 建立关联(association)，因此，和 AP 建立关联就像在总线型以太网中将终端连接到总线上。AP 和终端成功建立关联的先决条件是：

(1) AP 和该终端之间完成信道同步过程；

(2) AP 和该终端支持的物理层标准和传输速率存在交集；

(3) AP 完成对该终端的认证；

(4) AP 和该终端的 SSID 匹配；

(5) AP 具有的资源允许该终端接入 BSS。

终端从进入 BSA，到成功建立和 AP 之间的关联，允许和 AP 之间交换数据的过程如图 5.9 所示，这个过程等同于以太网的物理连接过程，无线局域网通过图 5.9 所示的过程，完成对终端的接入控制。首先，终端和 AP 之间通过交换探测请求和探测响应帧，完成信道和物理层标准同步过程，双方就通信使用的信道，物理层标准及数据传输速率达成一致。然后，由 AP 完成对终端的认证，图 5.9 中采用基于 MAC 地址的认证机制，只有 MAC 地址包含在 AP 授权终端地址列表中的终端，才能和 AP 建立关联。终端通过认证



图 5.9 建立关联过程

后，向 AP 发送关联请求帧(Association Request)，关联请求帧中除了需要给出终端的一些功能特性，如是否支持查询，是否进入 AP 的查询列表，和终端支持的传输速率外，还需给出终端的服务集标识符(Service Set Identifier，SSID)。SSID 用于标识某个基本服务集(BSS)，某个终端只有拥有了标识某个 BSS 的 SSID，才拥有接入该 BSS 的权利。AP 对这些信息进行分析，确定是否和该终端建立关联，如果 AP 确定和该终端建立关联，向该终端回送一个表示成功建立关联的关联响应帧(Association Response)，关联响应帧中给出关联标识符。否则，向终端发送分离帧(disassociation)。AP 在和该终端建立关联后，在关联表中添加一项，该项内容包含终端的 MAC 地址、认证方式、是否支持查询、支持的物理层标准、数据传输速率和关联寿命等，关联寿命给出终端不活跃时间限制，只要终端持续不活跃时间超过关联寿命，终端和 AP 的关联自动分离。就像总线型以太网中只有连接到总线上的终端才能进行数据传输一样，BSS 中只有 MAC 地址包含在关联表中的终端才能和 AP 交换数据。

5.3　WEP 的安全缺陷

802.11 最初的应用是解决类似手持式条形码扫描仪这样的移动设备和后台服务器之间的通信问题，而手持式条形码扫描仪这样的移动设备的处理能力非常有限，无法进行复杂的加密、解密计算，因此，只能采用 WEP 这样简单而有效的安全机制，这种安全机制在 802.11 最初的应用环境中也基本能够满足安全通信要求。但在笔记本计算机通过无线局域网访问内部网络的应用环境中，WEP 这样简单的安全机制将带来严重的安全问题，WEP 的安全缺陷开始显现。

5.3.1　共享密钥认证机制的安全缺陷

如图 5.10 所示，如果非授权终端(入侵终端)想通过 AP 的共享密钥认证过程，它可以一直侦听其他授权终端进行的共享密钥认证过程。因为无线电通信的开放性，入侵终端可以侦听到授权终端和 AP 之间共享密钥认证过程中相互交换的所有认证请求、响应

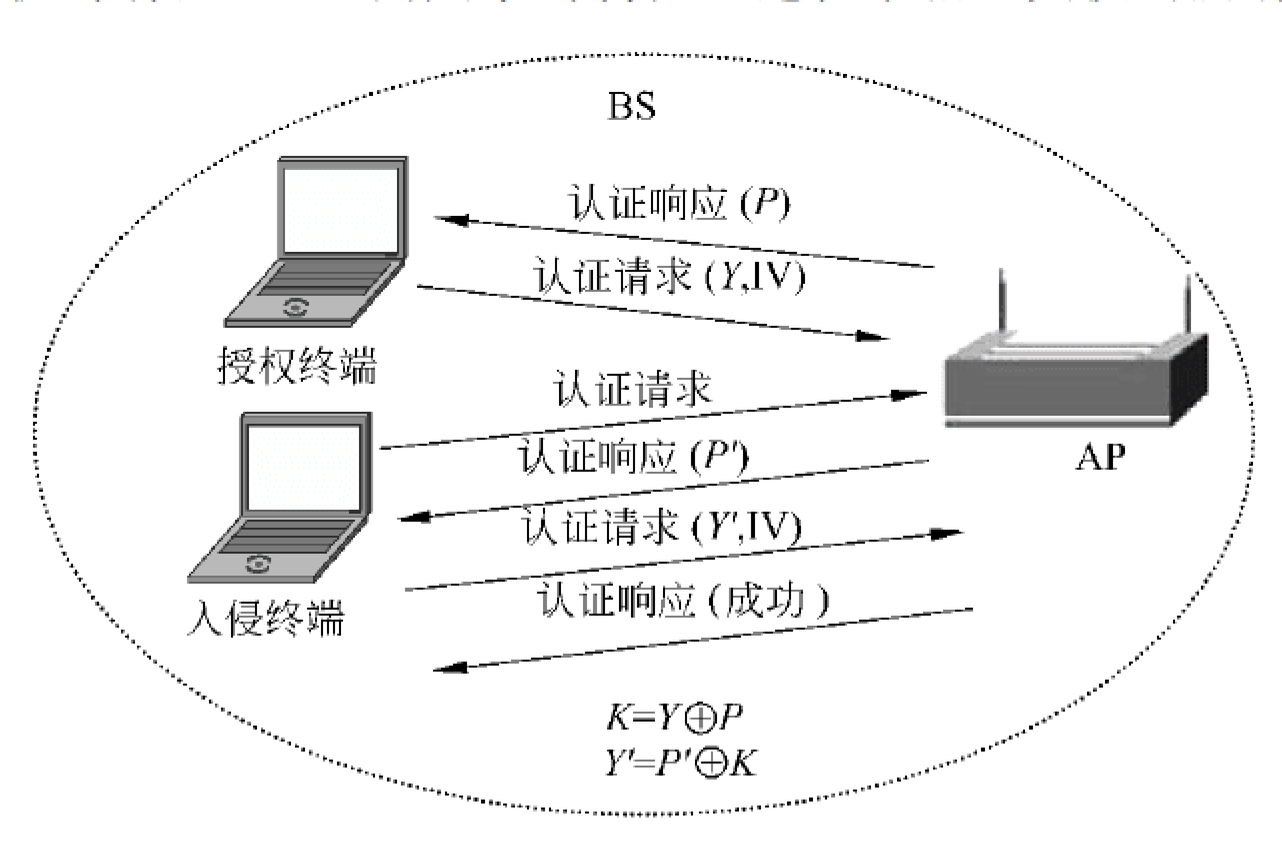


图 5.10　入侵终端通过 AP 认证的过程

帧。由于密文是通过一次性密钥和明文异或操作后得到的结果，$Y=K\oplus P$（Y 为密文，K 为一次性密钥，P 为明文），因此，用明文和密文异或操作后得到的结果即为一次性密钥 K，$Y\oplus P=K\oplus P\oplus P=K$。由于入侵终端侦听到了 AP 以明文方式发送给授权终端的随机数 P，和授权终端发送给 AP 的对随机数 P 加密后的密文 Y，入侵终端完全可以得出授权终端用于此次加密的一次性密钥 K 和对应的初始向量 IV。当入侵终端希望通过 AP 认证时，它也发起认证过程，并用侦听到的一次性密钥 K 加密 AP 给出的随机数 P'，并将密文 Y'（$Y=K\oplus P'$）和对应的初始向量 IV 封装成如图 5.4 所示的加密后的数据格式发送给 AP。由于入侵终端使用的一次性密钥 K 和初始向量 IV 都是有效的，AP 通过对入侵终端的认证。

5.3.2 一次性密钥字典

只要所有 BSS 中的授权终端都能保护好它们的密钥，入侵者想要获得某个 BSS 使用的密钥是困难的，但只要同时拥有明文和密文，就可得出一次性密钥。虽然不能通过一次性密钥推导出密钥，但相同数据长度下，最多只有 2^{24} 个一次性密钥，且这些一次性密钥和初始向量一一对应。因此，可以建立指定数据长度下的一次性密钥字典，字典中给出一次性密钥和初始向量之间的关联。但由于同一初始向量下，不同数据长度所对应的一次性密钥是不同的，因此，还须把一次性密钥字典中初始向量和一次性密钥之间的关联，从固定数据长度扩展到多个不同的数据长度。一旦建立每一个不同的初始向量和在不同数据长度下的一次性密钥之间的关联，入侵者就可根据侦听到的密文和初始向量，获得用于这一次数据加密的一次性密钥，并因而获得数据的明文。

图 5.11 是入侵者建立固定数据长度下一次性密钥字典的过程，连接在有线网络上的入侵者同伴反复向某个无线局域网中的授权终端发送固定长度的数据帧，入侵终端通过侦听 AP 发送给该授权终端的密文，逐步建立初始向量和一次性密钥之间的关联。假定无线局域网的传输速率为 11Mb/s，每一帧 MAC 帧的长度为 100B=800b，24 位 IV 对应 2^{24} 种不同的组合，无线局域网传输完 2^{24} 帧不同的 IV 组合对应的 MAC 帧所需要的时间约等于 $2^{24}/(11\times10^{6}/800)=1220\text{s}$，因此，建立固定数据长度的一次性密钥字典并不需要太长的时间。当入侵者希望得出不同数据长度下和某个初始向量关联的一次性密钥时，

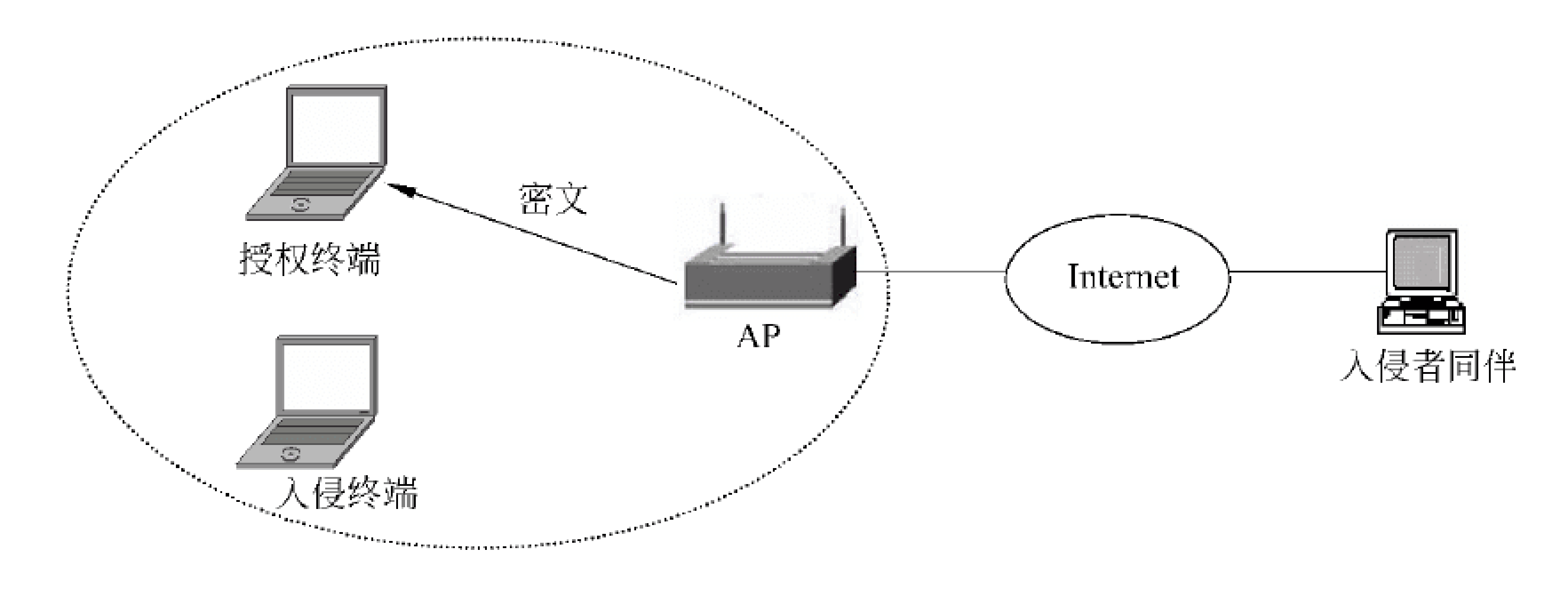


图 5.11 建立固定数据长度的一次性密钥字典

采用图5.12所示的过程。假定入侵者已经获得初始向量IV对应的长度为L(L单位为位)的一次性密钥K,希望求出初始向量IV对应的长度为$L+8$(数据长度以字节为单位)的一次性密钥K',其过程如下。入侵者构建长度为$L+8$的ICMP ECHO请求报文,由于入侵者只有长度为L(L单位为位)的一次性密钥K,K'的低8位是未知的。但8位二进制数只有256种可能,可以通过穷举法来求出低8位的正确值。K'的高L位固定为K,低8位值从0开始测试,每一次测试值作为一次性密钥加密ICMP ECHO请求报文,并将加密后的ICMP ECHO请求报文发送给AP,如果AP接收到正确的ICMP ECHO请求报文,将回送一个ICMP ECHO响应报文,只要接收到AP回送的ICMP ECHO响应报文,表明低8位测试值就是一次性密钥的低8位值,入侵者求得初始向量IV对应的长度为$L+8$的一次性密钥。这种过程可以一直进行,直到求出初始向量IV对应的任意长度的一次性密钥。

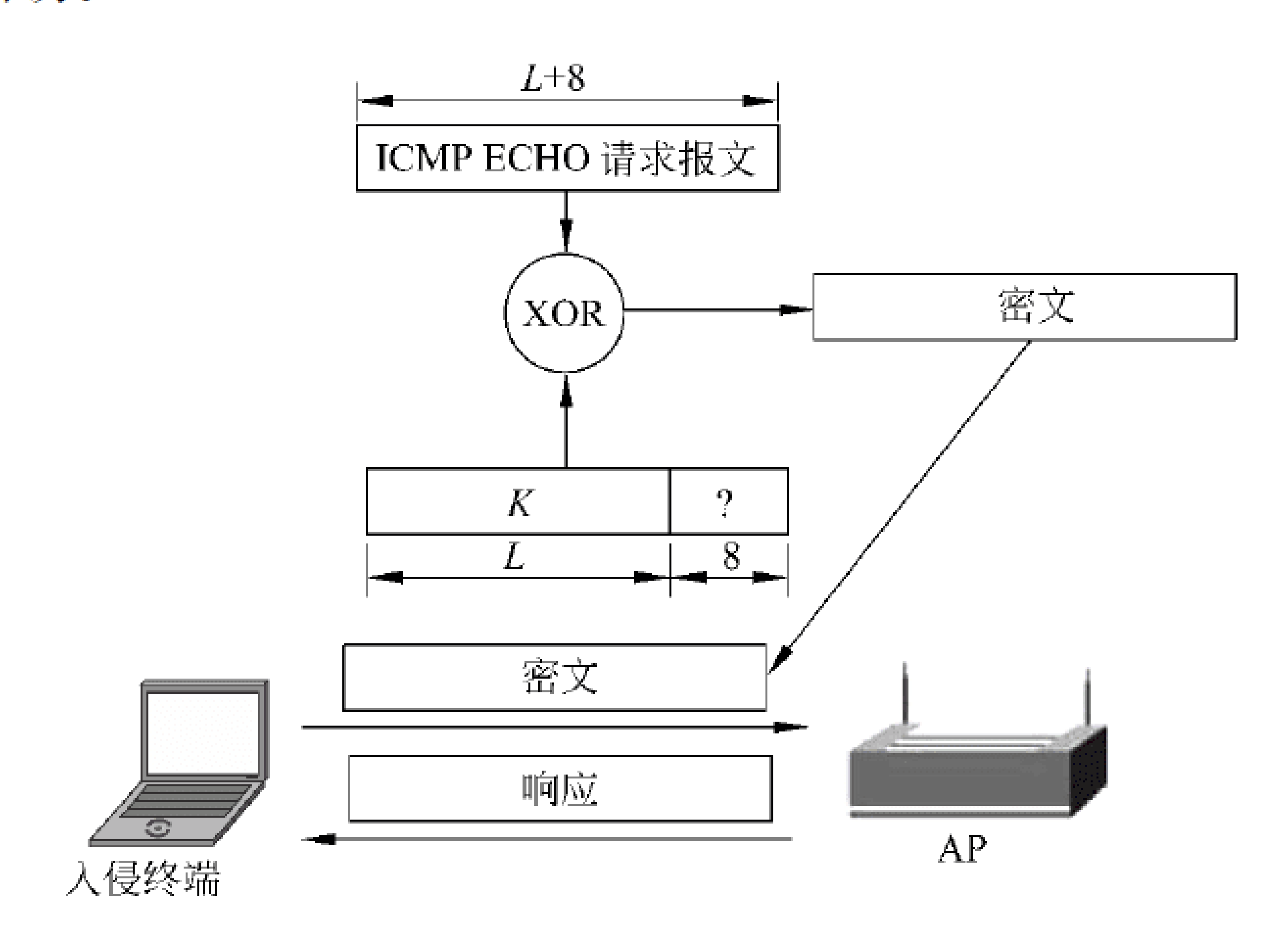


图5.12　扩展一次性密钥过程

5.3.3　完整性检测缺陷

假定数据1=$M_1(X)$,数据2=$M_2(X)$,生成函数=$G(X)$,如果$M_1(X)$和$M_2(X)$的阶数相同,且$R_1(X)$是$X^K\times M_1(X)/G(X)$的余数,$R_2(X)$是$X^K\times M_2(X)/G(X)$的余数,如果$M_3(X)=M_1(X)\oplus M_2(X)$,则$(R_1(X)\oplus R_2(X))$就是$X^K\times M_3(X)/G(X)$的余数。由于ICV就是数据除以生成函数后得到的余数,当数据=$M_1(X)$时,ICV=$R_1(X)$,WEP加密后生成的密文分别是$Y_1=M_1(X)\oplus K_1$,$Y_2=R_1(X)\oplus K_2$。如果密文Y_1被篡改为$Y_1'=Y_1\oplus M_2(X)$,则只要将密文Y_2修改为$Y_2'=Y_2\oplus R_2(X)$,接收端仍然能够通过数据的完整性检测,即用接收到的数据明文和生成函数$G(X)$求得的余数和接收到的作为ICV的余数明文相同,整个过程如图5.13所示。

如图5.13所示,发送端需要发送的数据为10101,假定$G(X)=X^3+X+1$(1011),根据数据和生成函数$G(X)$计算ICV的过程如图5.14(a)所示,ICV为(10101000)/(1011)的余数101,用一次性密钥11011101加密后得到的密文为01110000。攻击者截获发送者发送的密文,如果他希望篡改密文,并且使接收端检测不到密文在传输过程中被篡改,攻

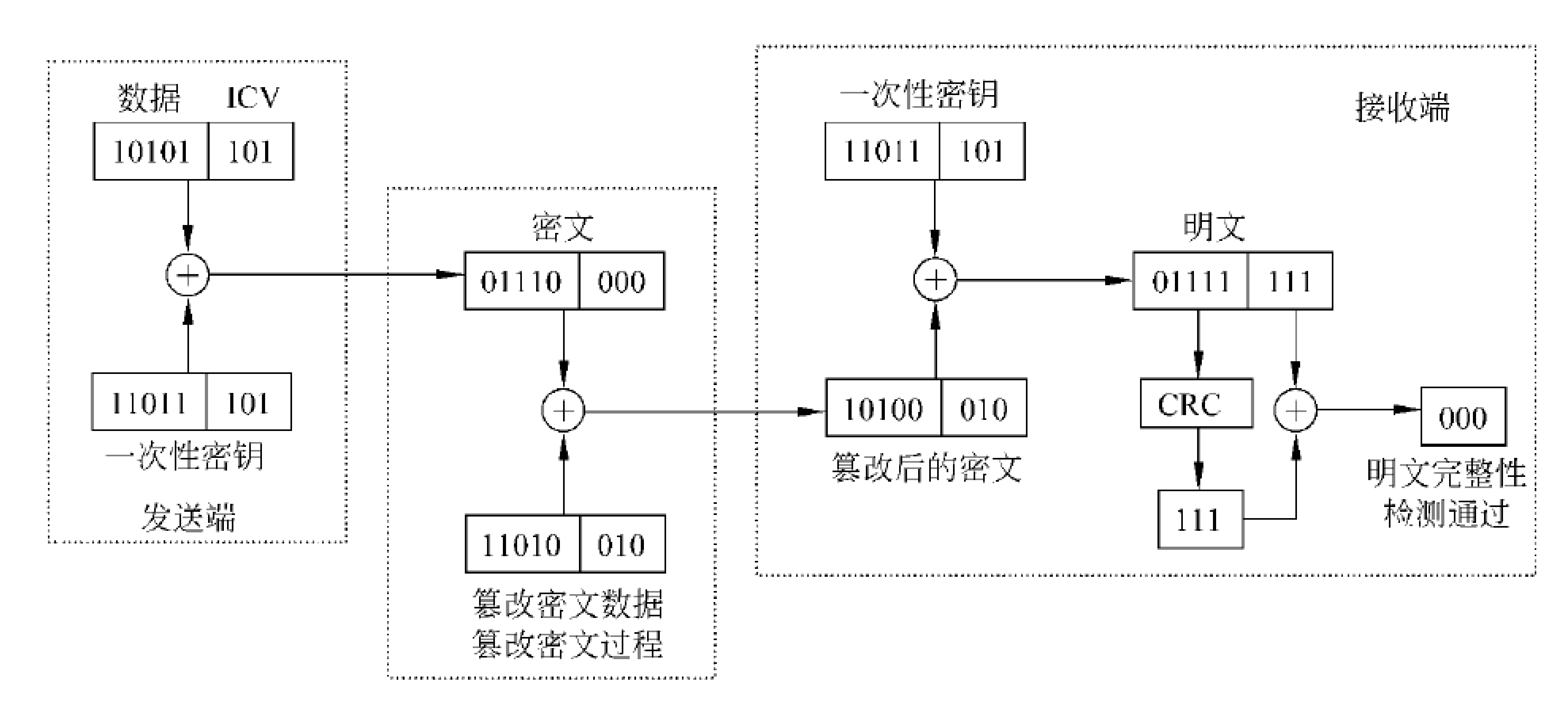


图 5.13 攻击者篡改密文过程

击者构建数据 11010，且根据数据 11010 和 $G(X)=X^3+X+1(1011)$ 计算 ICV，求得的 ICV 为 010，如图 5.14(b)所示。攻击者用和密文同样长度的数据序列 11010 010 和密文进行异或操作，得到篡改后的密文 10100 010。接收端接收到密文后，用和发送端相同的一次性密钥 11011101 对其进行异或操作，得到明文 01111 111，其中 01111 是数据，111 是用于检测数据完整性的 ICV，接收端根据数据 01111 和 $G(X)=X^3+X+1(1011)$ 计算 ICV，求得 ICV 为 111，如图 5.14(c)所示。接收端发现计算所得的 ICV 和 MAC 帧携带的 ICV 相同，认为密文在传输过程中未被篡改，作为正确数据予以接收，ICV 的完整性检测功能失去作用，这就是用根据数据和生成函数 $G(X)$ 计算所得的循环冗余检验码作为数据完整性检验值的缺陷，攻击者很容易篡改密文，又不被完整性检验值检测出。

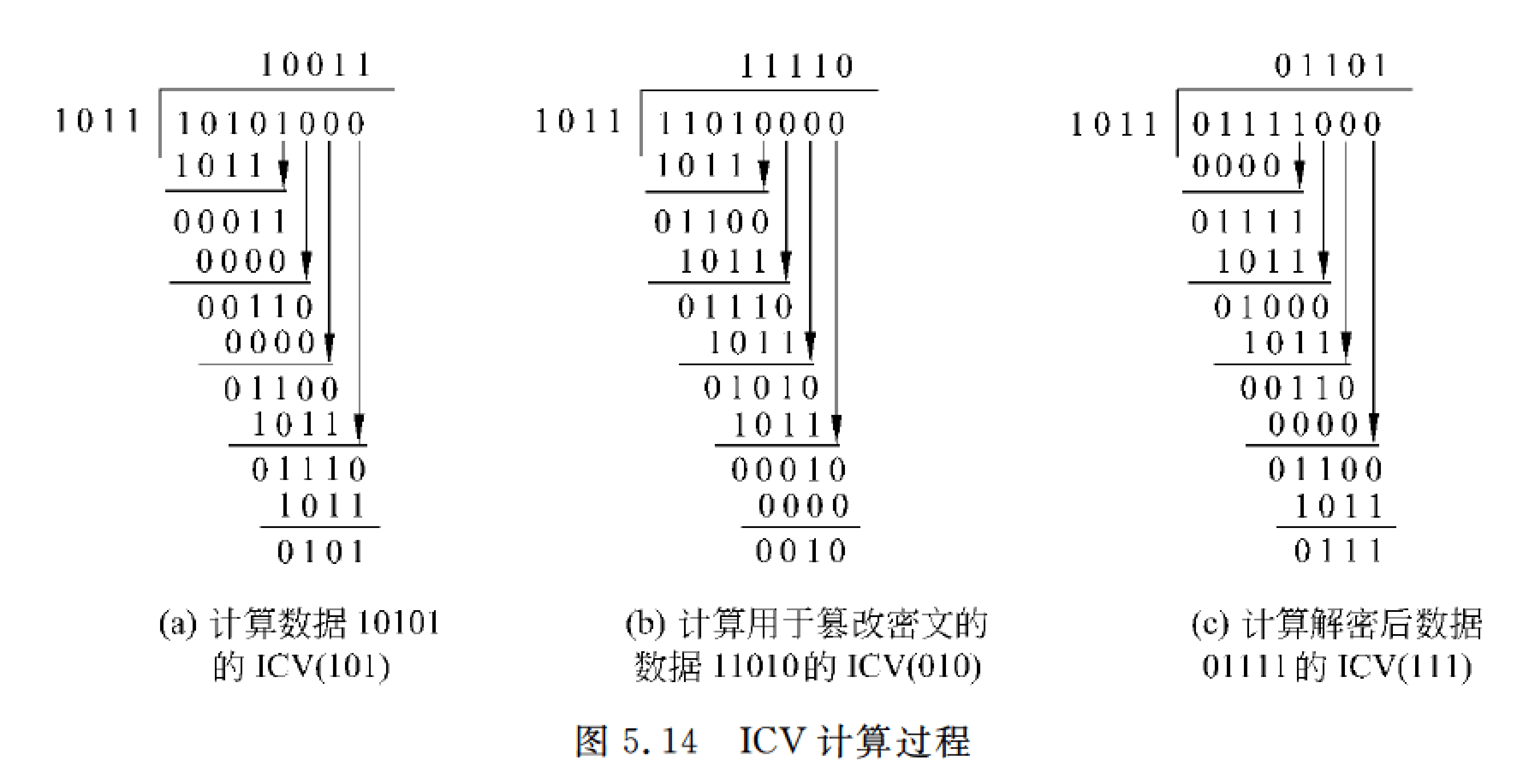


图 5.14 ICV 计算过程

5.3.4 静态密钥管理缺陷

属于同一 BSS 的终端共享同一密钥(或共享 4 个密钥)，由于一次性密钥只与 IV 和密钥相关，因此，属于同一 BSS 中的终端在密钥保持不变的情况下，只能共享 2^{24} 个一次性密钥，重复使用一次性密钥的几率大增，这将严重影响数据传输安全。另外，如果某台

设置了密钥的笔记本计算机失窃，或者某个知道密钥的人员离开原来的岗位，需要重新对所有属于同一 BSS 的终端配置新的密钥，这有可能是一件十分烦琐的工作。理想的密钥管理机制是基于用户，而不是终端分配密钥，这样，不同的用户即使使用同一终端，也要使用不同的密钥，同一用户即使使用不同的终端，也可使用同一密钥。密钥只和用户关联，和终端脱钩。

从以上的分析可以看出，WEP 安全机制根本无法满足数据通信网络的安全要求，因此，如果无线局域网和以太网一样成为目前 Internet 的有机组成部分，必须使用比 WEP 更强的加密和认证机制。

5.4 802.11i

WEP 的加密和认证机制存在重大缺陷，使得无线局域网无法满足数据通信的安全要求，严重制约了无线局域网的发展。随着笔记本计算机的普及和基于无线局域网的 VOIP 应用的开展，人们对移动通信的需求越来越大，因此，迫切需要一种满足无线局域网数据通信安全要求的加密和认证机制，以此促进无线局域网的发展和普及，这种新的、能够满足数据通信安全要求的加密和认证机制就是 802.11i。

5.4.1 802.11i 加密机制

802.11i 加密机制用于实现无线局域网环境下数据传输的保密性和完整性，目前 802.11i 定义了两种加密机制，分别是临时密钥完整性协议（Temporal Key Integrity Protocol，TKIP）和 CCMP(CTR with CBC-MAC Protocol)。

1. TKIP

WEP 加密机制的主要缺陷在于：

- 静态配置密钥；
- 属于同一 BSS 的所有终端共享 2^{24} 个一次性密钥；
- 不可靠的完整性检测机制。

因此，TKIP 一方面尽量与 WEP 加密机制兼容，以便快速更新无线局域网设备的安全机制，另一方面必须消除 WEP 加密机制的安全缺陷。它和 WEP 加密机制的不同之处在于如下几个方面：

临时密钥(Temporal Key，TK)和 WEP 加密机制中的密钥不同，一是 TK 是基于用户，而不是基于终端，二是 TK 在建立终端和 AP 之间的安全关联时产生，在该安全关联分离后删除，意味着每一次建立安全关联时都将产生不同的 TK。建立安全关联的过程在下一节详细讨论，注意，这里的安全关联是建立 AP 和终端之间能够更安全地交换数据的关联，不是 IPSec 的安全关联。

TKIP 用 48 位的序号计数器(TKIP Sequence Counter，TSC)取代 WEP 的 24 位初始向量(IV)，而且由于发送端地址参与加密每一帧的一次性密钥的产生，每一个发送端都有单独的 48 位序号空间，这不仅大大增加了一次性密钥的空间，保证在任何安全关联存在期间都不会使一次性密钥重复，而且还可以用序号防止中继攻击(亦称重放攻击)。

TKIP 采用 Michael 算法计算消息完整性编码(Message Integrity Code,MIC),这是一种类似于 HMAC 的算法,但比 HMAC-MD5 或 HMAC-SHA-1 简单,它对数据进行基于 MIC 密钥的报文摘要计算,产生 8 字节的 MIC,一旦数据被篡改,重新计算出的 MIC 将发生改变。

图 5.15 是 TKIP 的加密过程,48 位的 TSC 的初始值为 1,发送端每发送一帧 MAC 帧,将 TSC 增 1。在加密过程中,TSC 被分成高 32 位和低 16 位两部分,高 32 位和 128 位的临时密钥 TK、48 位的发送端地址 TA 一起作为第 1 级密钥混合函数的输入,用于产生 80 位的中间密钥 TTAK,TTAK、TK 和 TSC 的低 16 位一起作为第 2 级密钥混合函数的输入,用于产生 128 位的 WEP 伪随机数种子,第 1 级和第 2 级密钥混合函数的功能类似于伪随机数生成器,一是无法通过输出推导出输入,二是输入的改变会尽量影响输出的改变。对于 WEP 加密算法而言,128 位伪随机数种子由 104 位的 WEP 密钥和 24 位的初始向量组成,而第 2 级密钥混合函数的输出是 112 位的 WEP 密钥和 TSC 的低 16 位,以此构成 128 位的 WEP 伪随机数种子。将产生 WEP 伪随机数种子的过程分成两级是既要增加用于加密每一帧 MAC 帧中数据的一次性密钥的空间,又要尽可能减少计算的复杂性,对于两级计算过程,在 TSC 高 32 位维持不变的情况下,中间密钥 TTAK 是不变的,这就意味着每发送 2^{16} 帧 MAC 帧,才需要重新计算一次 TTAK。由于每发送一帧 MAC 帧,都将 TSC 增 1,因此,每一次发送 MAC 帧,都需重新计算 WEP 伪随机数种子,保证每一帧 MAC 帧对应的 WEP 伪随机数种子都不同,导致用于加密该帧数据的一次性密钥也不同。作为 MAC 帧净荷的服务数据单元(MSDU)和该 MAC 帧的源 MAC 地址(SA)、目的 MAC 地址(DA)和 1B 的优先级串接在一起,构成数据序列作为 Michael 函数的输入,1B 的优先级目前没有定义,其值固定为 0。Michael 基于 MIC 密钥计算数据序列的报文摘要,产生 8B 的 MIC。作为 Michael 函数输入的数据序列和 MIC 串接在一起作为 WEP 加密算法的 MSDU,如果需要的话,可以将 MSDU 分段,分段后的每一段数据作为 WEP 加密算法的 MSDU,如图 5.16 所示。WEP 加密算法根据 MSDU 和生成函数 $G(X)$产生 ICV,同时根据 WEP 伪随机数种子生成长度为 MSDU+ICV 的

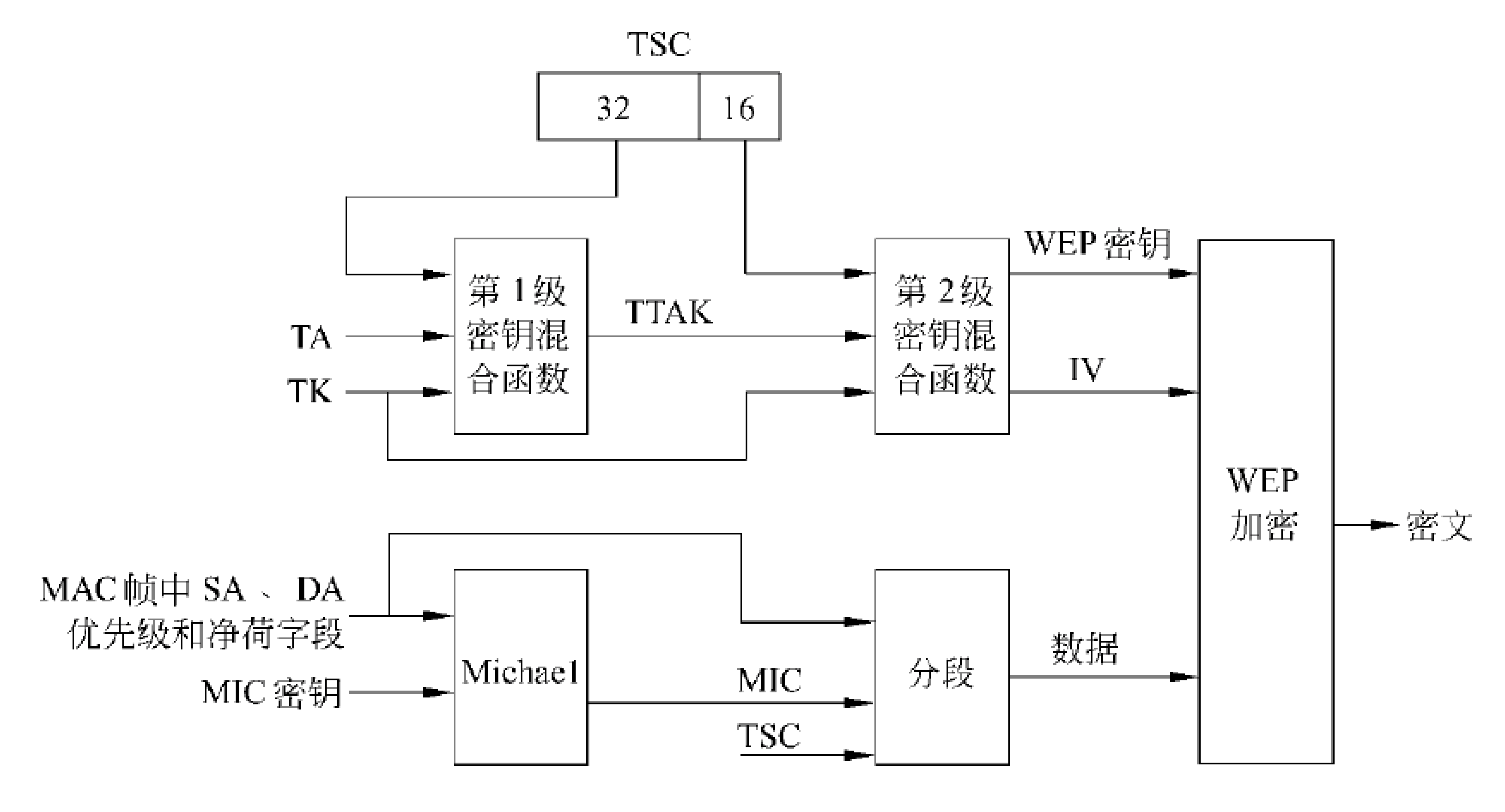


图 5.15　TKIP 加密过程

一次性密钥，一次性密钥和(MSDU‖ICV)异或操作后产生密文，用密文作为协议数据单元(MPDU)的净荷构成发送端用于发送的MAC帧，WEP加密算法的操作过程和图5.4所示的过程相同，TKIP MPDU封装过程如图5.16所示。

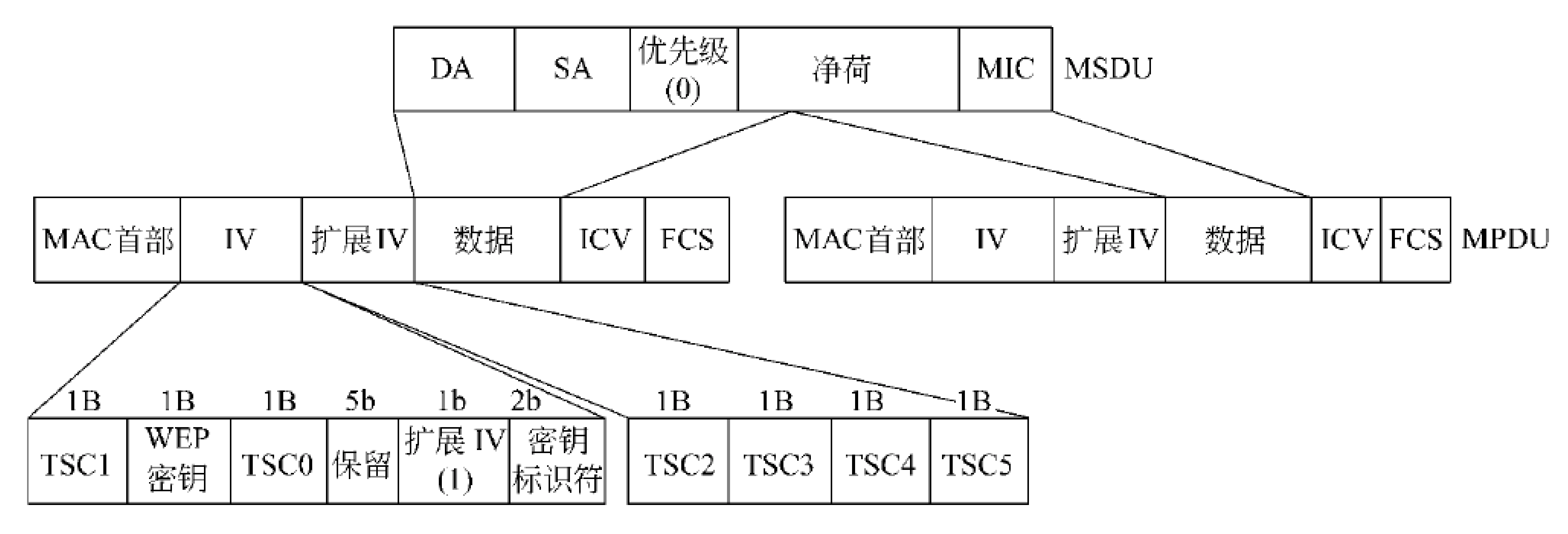


图5.16 TKIP MPDU封装过程

由于发送端为每一个安全关联配置TSC，而且，发送端每向安全关联的另一端发送一帧MAC帧后，将TSC增1，因此，接收端可用接收到的MAC帧所携带的TSC进行中继攻击(亦称重放攻击)检测。接收端同样对每一个安全关联设置一个中继计数器(亦称重放计数器)，如果成功接收一个MAC帧，就将该MAC帧携带的TSC作为当前中继计数器值，当新接收到一帧MAC帧时，根据MAC帧的TA找到对应的中继计数器值，如果该MAC帧携带的TSC值大于中继计数器值，则进行后续处理，否则，丢弃该MAC帧，并作相应的出错处理。不同的TSC对应不同的WEP伪随机数种子，因而产生不同的一次性密钥，因此，TKIP的一次性密钥空间为2^{48}，而且，这样的一次性密钥空间只对应和某个安全关联相关的终端和AP(也可以是和某个安全关联相关的成对终端)，这种情况下，攻击者想要在发送端和AP的安全关联存在期间求出有效的一次性密钥字典是根本不可能的事，数据传输的保密性得到保证。

发送端和接收端成功交换数据的前提是拥有相同的临时密钥TK，当接收端接收到MAC帧时，从MAC帧中分离出TA和TSC，根据TA找到对应的TK，和发送端同样的方法计算出WEP伪随机数种子，通过图5.5所示的解密过程得出数据和ICV明文，根据数据和生成函数$G(X)$重新计算ICV，将计算所得的ICV和MAC帧携带的ICV比较，如果相同，该MAC帧成功接收，MAC帧携带的TSC值作为该TA对应的中继计数器值，否则，丢弃该MAC帧，并作相应的出错处理。如果该MAC帧携带的数据是完整的MSDU，则直接进行完整性检测，如果该MAC帧携带的数据是分段后的某个数据段，则等待所有数据段全部成功接收，并将这些数据段拼装为原始MSDU后进行完整性检测。Michael函数将MSDU中的SA、DA、优先级和数据进行基于MIC密钥的报文摘要运算，得出8B的MIC，将重新计算所得MIC和MSDU中的MIC进行比较，如果相等，表示完整性检测正确，否则进行对应的出错处理。TKIP解密过程如图5.17所示。

由于Michael函数是类似HMAC的基于密钥的报文摘要算法，虽然其运算过程和HAMC-MD5、HAMC-SHA-1相比要简单得多，但攻击者很难通过同时篡改数据序列和MIC使数据完整性检测失效，无线局域网数据传输的完整性得到保证，另外，由于数据序

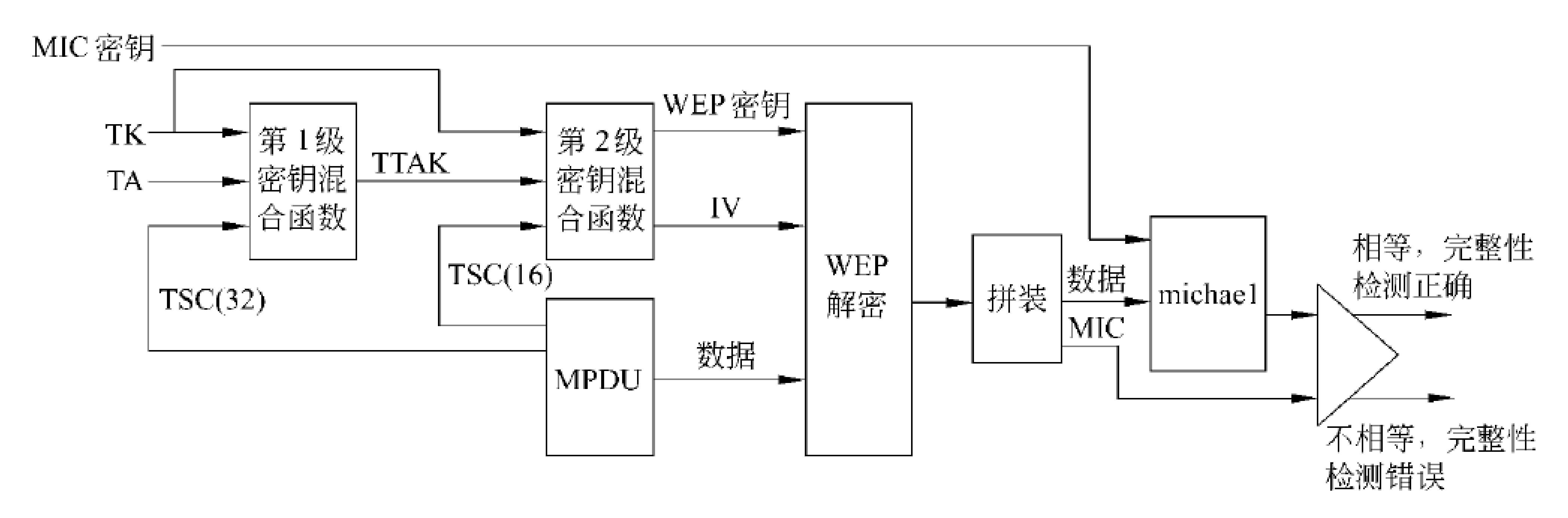


图 5.17 TKIP 解密过程

列中包含了源和目的 MAC 地址，使得源地址欺骗攻击难以实现。

2. CCMP

1）CCMP 加密和完整性检测机制

3.1.1 节中介绍了两种密码体制：流密码和分组密码体制，如果流密码体制中的一次性密钥空间无限大，而且，用于加密每一帧 MAC 帧的一次性密钥完全随机产生，各个一次性密钥之间没有任何相关性，流密码体制的安全性是非常好的，但这两个前提往往很难做到，对于 WEP 和 TKIP 这样的流密码体制，一是一次性密钥空间总是有限的，WEP 的一次性密钥空间是 2^{24}，TKIP 是 2^{48}。二是用于加密每一帧 MAC 帧的一次性密钥由伪随机数生成器根据输入的伪随机数种子计算得到的，伪随机数种子和一次性密钥一一对应，由于伪随机数生成器的算法是公开的，而且为了在发送端和接收端之间同步一次性密钥，一部分伪随机数种子以明文的方式包含在发送端传输给接收端的 MAC 帧中，攻击者能够通过截获到的一些一次性密钥及其对应的 IV 或 TSC，推导出 WEP 密钥或临时密钥 TK，从而攻破 WEP 或 TKIP 的安全机制。分组密码体制的好处在于加密算法的安全性，即在截获到多组密文及对应的明文后，也无法推导出密钥，因此，密钥的安全性好于 WEP 和 TKIP，但加密算法的复杂性要高于 WEP 或 TKIP 的伪随机数生成算法。

CCMP MIC 算法如图 5.18 所示，标志字节给出有关 MIC 长度和随机数长度的一些

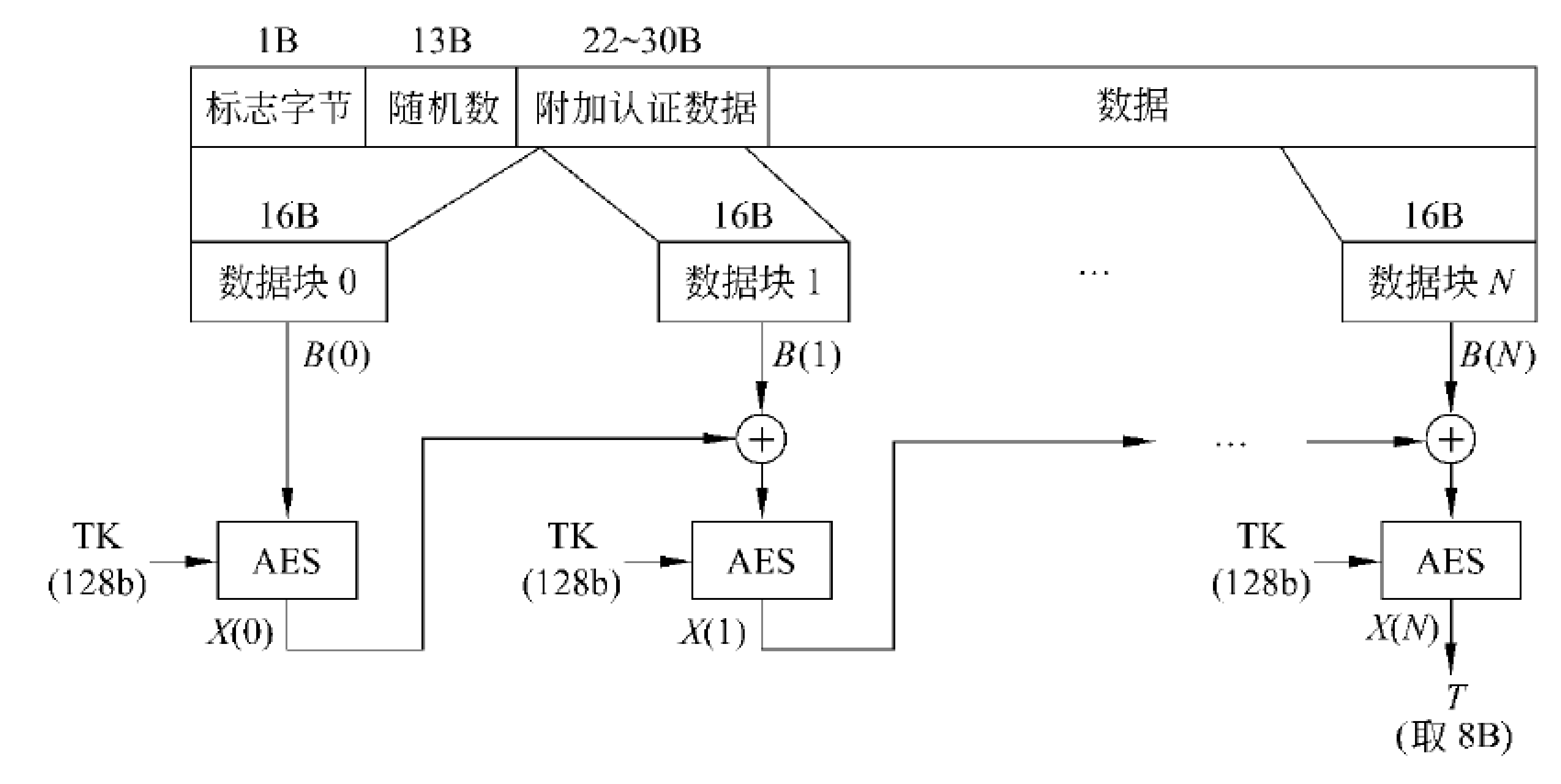


图 5.18 MIC 算法

信息。在用于实现无线局域网环境下的数据完整性检测时，附加认证数据由无线局域网 MAC 帧首部中的不变字段值组成，13B 的随机数也由一些和安全关联相关的参数组成。CCMP 工作过程中将对它的构成进行说明。CCMP MIC 算法首先将需要进行完整性检测的数据序列分成长度为 16B 的数据块（$B(0)$、$B(1)\cdots B(N)$），然后对数据块进行加密分组链接运算，具体运算过程如下：

$$X_0=\mathrm{AES}(\mathrm{TK},B(0))$$
$$X_1=\mathrm{AES}(\mathrm{TK},X_0\oplus B(1))$$
$$\vdots$$
$$X_N=\mathrm{AES}(\mathrm{TK},X_N-1\oplus B(N))$$
$$T=X_N\text{ 的高 64 位}$$

CCMP 加密算法如图 5.19 所示，由 1B 标志字节、13B 随机数和 2B 计数器值构成一个数据块，其中标志字节给出有关随机数和计数器长度的信息，这里确定随机数长度为 13B，计数器长度为 2B。数据块 $A(i)$ 的计数器值为 i。在用于实现无线局域网环境下的数据加密时，13B 随机数的构成和 MIC 算法相同。$S(i)=\mathrm{AES}(\mathrm{TK},A(i))$，其中 $S(0)$ 的高 64 位用于和 T 进行异或运算，产生 64 位的 MIC。$S(1)\parallel S(2)\cdots\parallel S(N)$ 串接为和数据同样长度的密码流，并和数据进行异或运算，产生密文。从 CCMP 加密算法可以看出，CCMP 用 AES 取代 WEP 和 TKIP 中的伪随机数生成算法，由于 AES 的安全性远高于伪随机数生成算法，因此，CCMP 加密算法和完整性检测算法的安全性均高于 TKIP，当然，CCMP 的计算复杂性也远高于 TKIP，具体选择时，需要在计算复杂性和安全性之间取舍。

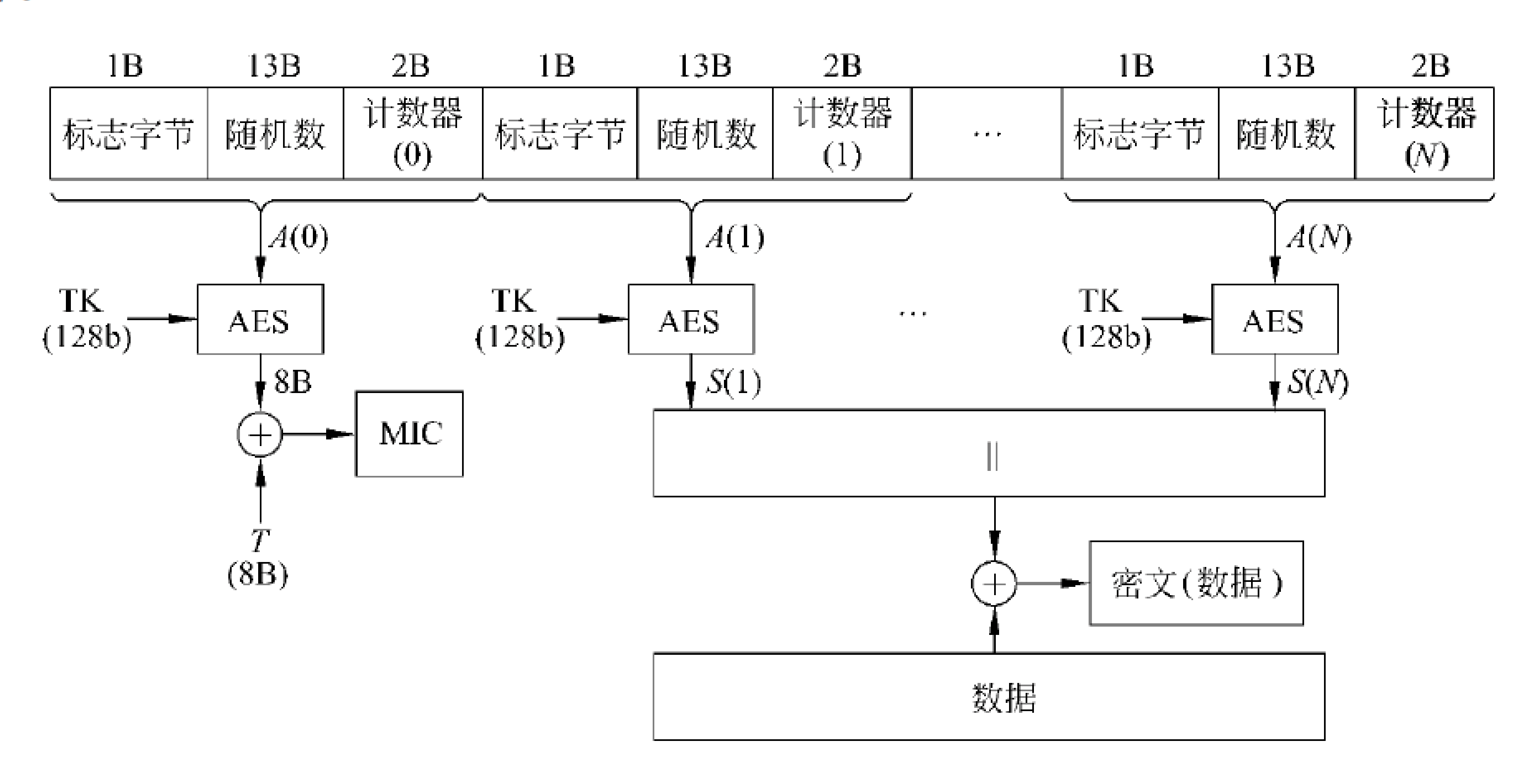


图 5.19　数据加密算法

2）CCMP 工作过程

发送端用 CCMP 加密数据的过程如图 5.20 所示，将 MAC 帧首部中需要在传输过程中保证完整性的字段作为图 5.18 中的附加认证数据，这些字段包括各种地址字段、控制字段及其他传输过程中保持不变的字段，这些字段用明文传输，但必须保证在传输过程没有被篡改。图 5.18 和图 5.19 中 13B 随机数由 6B 源地址（A_2），6B 报文编号（PN）和

1B 目前固定为 0 的优先级组成，发送端为每一个安全关联配置报文编号计数器，每发送一帧 MAC 帧，报文编号计数器增 1，因此，建立安全关联的终端和 AP 之间传输的每一帧 MAC 帧所对应的报文编号都不同，这一方面保证用不同的密钥流加密不同 MAC 帧，另一方面可以用报文编号检测中继攻击，可以看出，CCMP 的报文编号的含义和用途与 TKIP 的 TSC 相似。由于 CCMP 采用 AES 加密算法，因此，采用 128b 的临时密钥 TK。CCMP 首部字段如图 5.21 所示，它主要由 6B 的报文编号组成，但为了和 WEP MPDU 兼容，通过置位扩展 IV 位将 IV 字段扩展为 8B 后，作为 CCMP 首部。

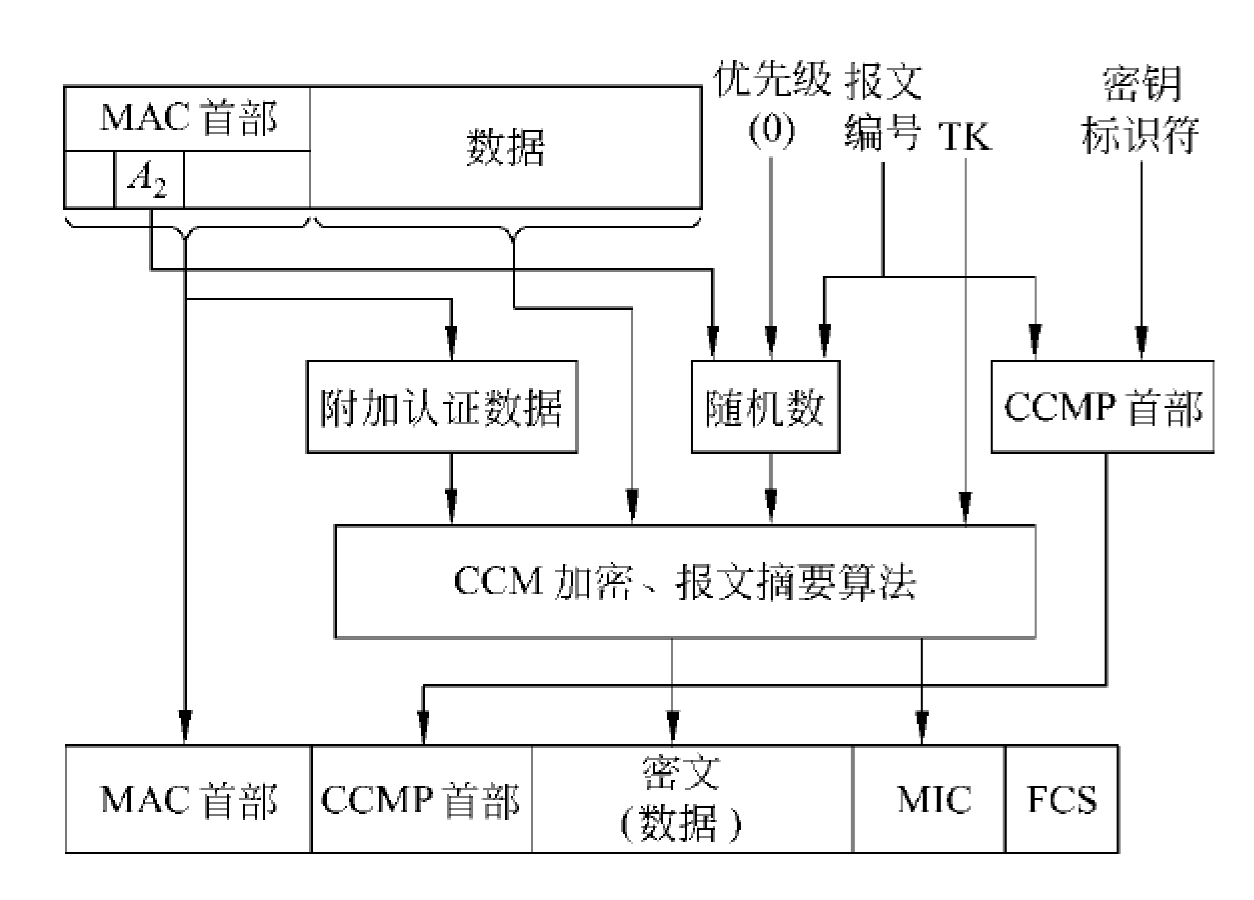


图 5.20　CCMP 加密过程

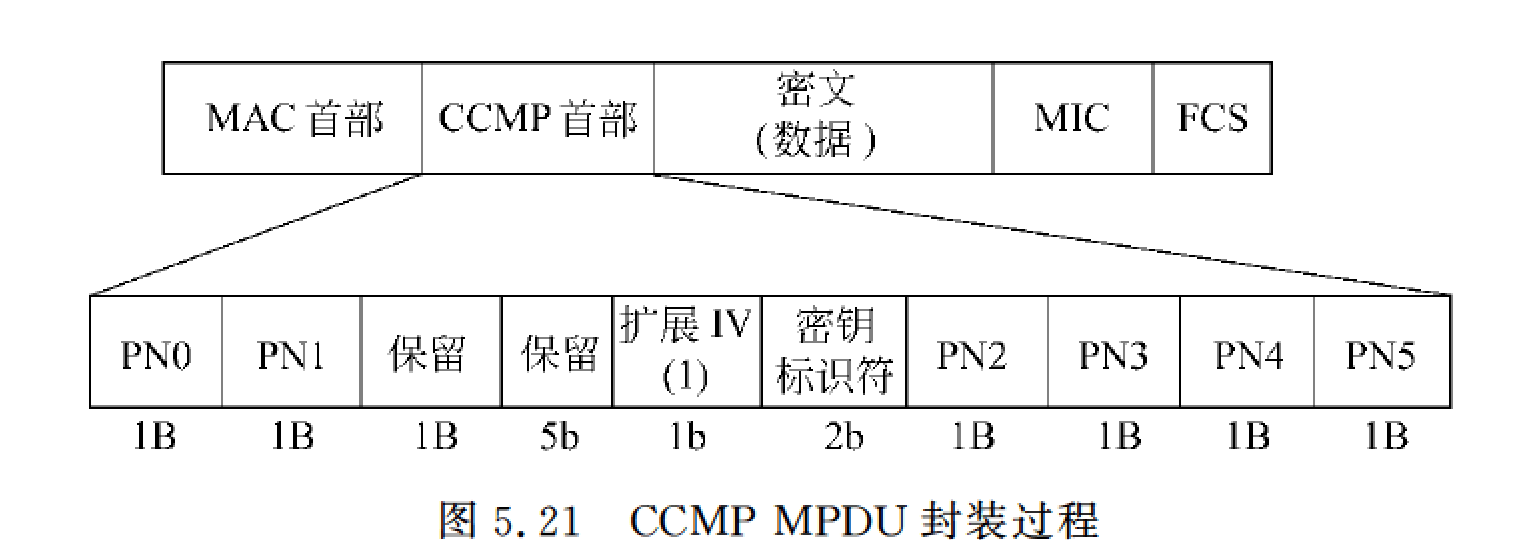


图 5.21　CCMP MPDU 封装过程

CCMP 解密和完整性检测过程如图 5.22 所示，接收端从 MAC 首部得到附加认证数据，从 CCMP 首部得到报文编号，报文编号和 A_2、固定为 0 的优先级一起组成随机数，CCMP 根据图 5.19 所示的密钥流生成过程生成密钥流，将其和 MAC 帧中的密文进行异或操作得到明文，同时根据 MAC 帧中的 MIC 还原出图 5.18 所示的 T。将附加认证数据和明文重新构成图 5.18 所示的数据序列，并计算出 T，将计算出的 T 和根据 MAC 帧中 MIC 还原出的 T 比较，如果相同，完整性检测正确，否则，丢弃该 MAC 帧。和 TKIP 一样，每一个安全关联都配置中继计数器，正确接收的 MAC 帧的报文编号作为中继计数器的当前值，如果新接收到的 MAC 帧的报文编号大于中继计数器的值，表示该 MAC 帧不是用于中继攻击的 MAC 帧，继续处理该 MAC 帧，否则，丢弃该 MAC 帧，并作相应的出错处理。

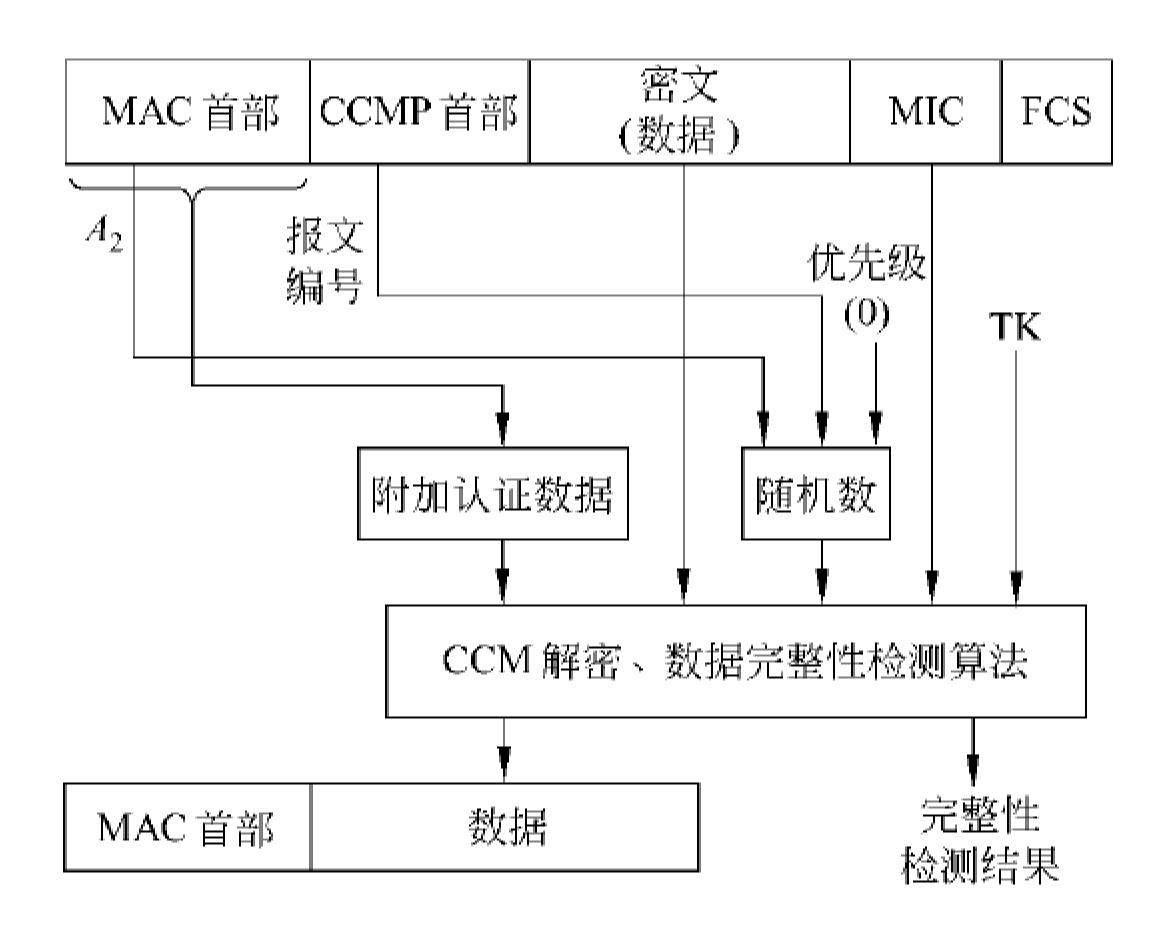


图 5.22　CCMP 解密和完整性检测过程

5.4.2　802.1X 认证机制

AP 和终端之间建立关联的过程就像是将终端连接到以太网交换机中某个端口的物理连接过程，如果该以太网交换机端口不需要进行接入控制，终端一旦用双绞线电缆接入该以太网交换机端口，就完成了接入以太网的过程。同样，如果 AP 不对与某个终端之间的关联进行接入控制，终端一旦建立和 AP 之间的关联，也完成了接入无线局域网的过程。如果需要对某个以太网交换机端口进行接入控制，终端接入以太网交换机的端口后，并不能通过该端口输入输出数据，必须由该端口对接入用户进行认证，通过认证后，该端口才能正常转发终端的数据，3.4.3 节讨论的 802.1X 就是这样一种基于端口的接入控制协议。同样，如果需要 AP 对与某个终端之间的关联进行接入控制，AP 建立和该终端之间的关联后，也不能转发和该终端相关的数据，必须对接入用户进行认证，通过认证后，才能正常转发和该终端相关的数据。802.11i 下，AP 和终端之间的关联是受控的，刚建立时，关联处于非认证状态，相关终端不能通过 AP 转发数据，只有通过对用户的认证，关联才能从非认证状态转变为认证状态，相关终端才能通过 AP 正常转发数据。另外，802.11i下，密钥是基于用户，而不是基于终端，并且，每一次会话所使用的密钥均应不同，这也是临时密钥 TK 的本质含义，这样的密钥无法静态配置，必须在会话开始时动态分配，因此，802.11i 需要在关联建立后完成对接入用户的身份认证，并在通过接入用户的身份认证后为该接入用户动态分配临时密钥 TK，这种经过身份认证并动态分配临时密钥 TK 的关联称为安全关联，临时密钥 TK 只在安全关联存在期间有效，一旦该安全关联分离，或重新建立安全关联，必须重新分配临时密钥 TK。802.11i 也用 802.1X 作为接入控制协议，当然，802.11i 下，802.1X 基于关联对接入进行控制，如图 5.23 所示。

802.1X 用 EAP 作为认证协议，而 EAP 可以采用多种认证机制，不同认证机制适用不同的应用环境。802.1X 用于对接入以太网的终端进行接入控制时，往往只需对用户进行认证，以便计费和管理，因此，用 CHAP 作为认证机制。但在无线通信环境下，为了保

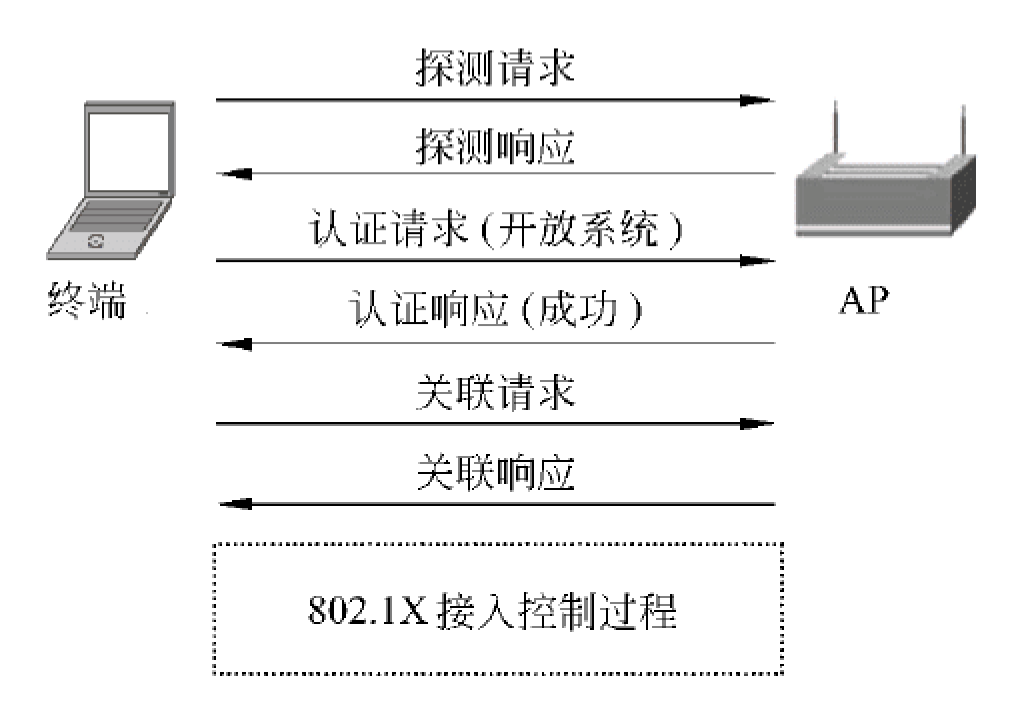


图 5.23 关联建立过程

证安全,不仅需要对接入用户进行认证,用户也需要通过认证 AP,保证接入的 AP 不是假冒的。因此,需要采用具有双向认证能力的认证机制。

建立安全关联的前提是终端和 AP 之间已经成功建立关联,为了和 802.11 兼容,在建立关联之前仍然需要完成对终端的认证,由于在建立安全关联时终端和 AP 之间需要进行更严格的双向认证过程,因此,建立关联之前的认证过程一般采用开放系统认证机制或基于 MAC 地址认证机制,图 5.23 是采用开放系统认证机制的关联建立过程。

终端和 AP 一旦启动安全关联机制,建立关联后,双方都不能通过关联传输数据,只有在各自完成对对方的身份认证后,关联才能从非认证状态转换为认证状态,另外,建立安全关联过程中必须为双方分配临时密钥 TK,该临时密钥 TK 一是只用于建立安全关联的终端和 AP 之间,二是只在该安全关联存在期间有效,因此,被称为成对临时密钥。为保证数据传输的保密性,即使是相同的终端和 AP 之间,不同时间建立的安全关联所对应的临时密钥 TK 必须不同。安全关联建立过程可以分为认证过程和密钥管理过程,它们都由 802.1X 实现,这一节讨论 802.1X 认证机制,下一节讨论 802.1X 密钥管理机制。

1. 双向 CHAP 认证机制

挑战握手认证协议(Challenge Handshake Authentication Protocol,CHAP)是一种单向认证协议,当认证者需要认证用户的身份时,向终端发送随机数 challenge,终端接收到认证者发送的 challenge 后,进行如下运算:

$$\text{MD5(标识符} \parallel \text{challenge} \parallel \text{口令)} \quad (5.1)$$

其中,标识符是认证者发送的用于传输 challenge 的 EAP 请求报文中的标识符字段值,口令由用户在认证过程中输入,它必须和认证数据库中该用户对应的口令相同,如图 5.24 中,用户 A 在认证过程中输入的口令必须是 PASSA。式(5.1)运算结果作为 challenge 响应通过 EAP 响应报文发送给认证者,认证者重新根据认证数据库中的口令运算式(5.1)的值,如果运算结果和客户发送的 challenge 响应相等,用户身份得到认证,否则,表示认证失败。单向认证过程用于确认用户是否拥有标识其身份的口令,如果用户需要确认认证者的身份,也需要确认认证者是否拥有标识自己身份的口令,因为口令只掌握在用户和

完成用户注册的认证者中。用户认证认证者的过程和认证者认证用户的过程相同，只是由终端首先通过 EAP 请求报文向认证者发送随机数 challenge，当然，终端向认证者发送的 challenge 和认证者向终端发送的 challenge 不同，由认证者根据认证数据库中用户 A 对应的口令运算式(5.1)的值，然后，将运算结果作为 challenge 响应通过 EAP 响应报文发送给终端，终端根据用户 A 输入的口令重新运算式(5.1)的值，如果运算结果和认证者发送的 challenge 响应相等，认证者身份得到确认；否则，表示认证失败。当然，对于图 5.24 所示的网络结构，认证过程在终端和认证服务器之间进行，AP 作为认证者只是用于转发认证过程中双方交换的报文，并实现 EAP 报文 MAC 帧封装格式和 RADIUS 报文封装格式之间的转换。用户 A 和认证服务器之间的双向 CHAP 认证过程如图 5.25 所示。相互完成对对方的身份认证后，终端和 AP 必须拥有成对主密钥(Pairwise Master Key，PMK)，认证服务器通过口令计算出 PMK，并作为属性值以密文方式通过 RADIUS 允许接入报文发送给 AP，终端必须能够通过用户 A 输入的口令计算出同样的 PMK，显然，PMK 是终端和 AP 的共享密钥，密钥管理机制必须根据 PMK 推导出临时密钥 TK，而且，对于终端和 AP 在不同时间建立的安全关联，密钥管理机制根据相同 PMK 推导出的临时密钥 TK 必须不同。

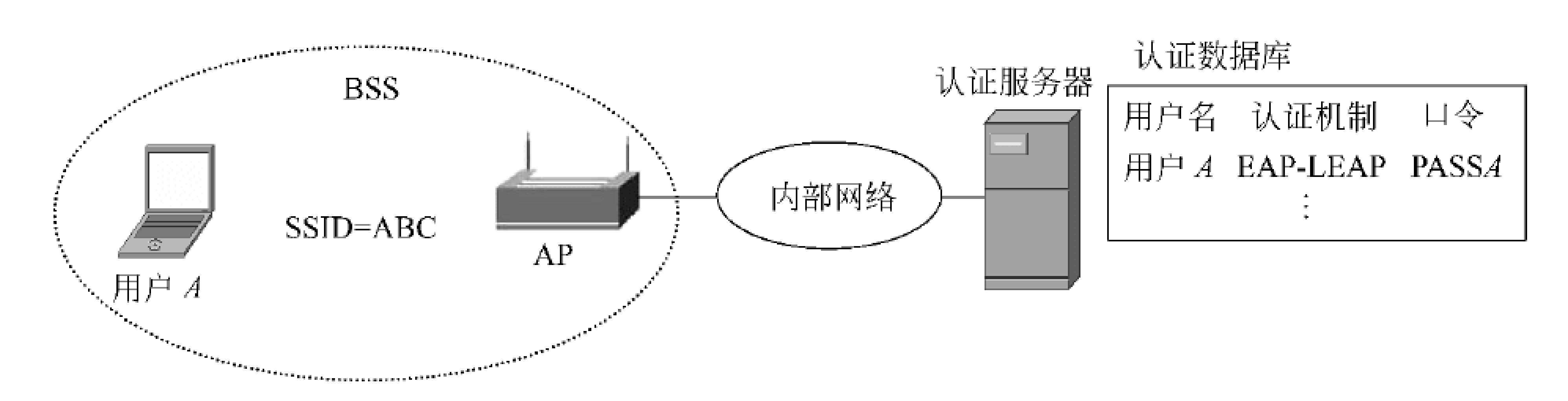


图 5.24　双向 CHAP 认证机制对应的网络结构

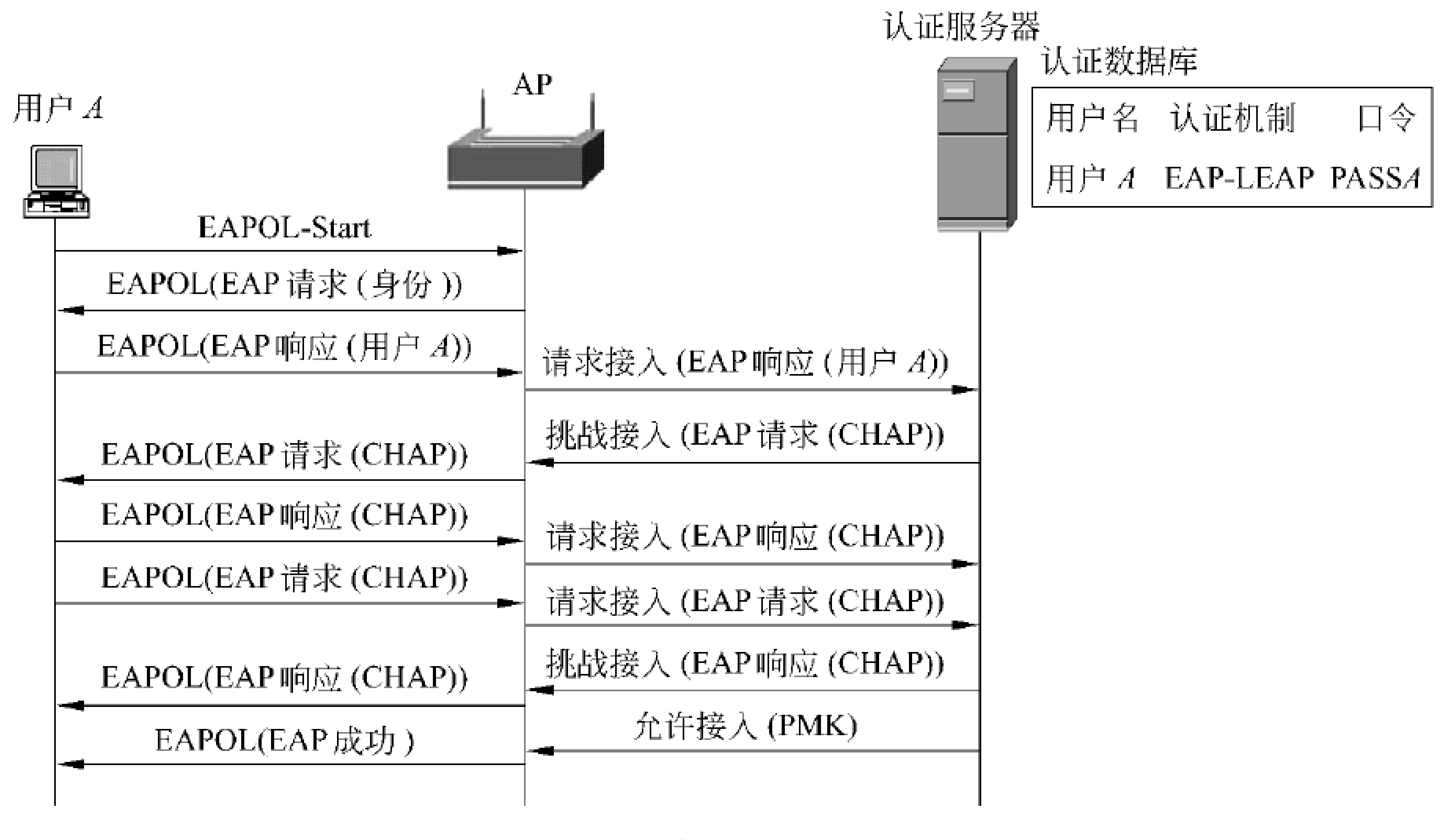


图 5.25　双向 CHAP 认证过程

2. EAP-TLS 认证机制

双向 CHAP 认证机制通过改进将 CHAP 的单向认证功能扩展为双向认证功能，但由于 CHAP 本身的安全性不是很高，导致双向 CHAP 认证机制的安全性受到限制。由于不存在标准的根据口令推导 PMK 的算法，双向 CHAP 认证机制的通用性不够，因此，不同厂家生产的采用双向 CHAP 认证机制的无线网卡、AP 和认证服务器很难兼容。目前，应用广泛且标准的双向认证机制是 EAP-TLS 认证机制，它主要通过数字签名技术进行身份认证。用数字签名技术认证身份的过程如下：首先需要提供由认证中心(CA)签发的用于证明用户和公钥之间关联的证书，当然，提供证书的同时，必须提供有关能够让双方对认证中心的权威性达成共识的证明材料。由于公钥和私钥是一一对应的，拥有私钥的用户就是证书中和公钥关联的用户，因此，某个用户只要提供了证明公钥 PKA 和用户 *A* 关联的证书，同时又能够证明拥有 PKA 对应的私钥 SKA，该用户就是用户 *A*。TLS 除了对双方身份进行认证外，还能够就双方采用的加密、解密算法及密钥达成共识。

当然，在无线局域网环境中，LAN 作为 EAP 的传输网络，EAP 采用 TLS 作为认证机制，因此，在无线局域网的 802.1X 中，用 EAP 报文封装 TLS 消息，同时又通过 EAPOL 封装过程将 EAP 报文封装成能够通过无线局域网传输的 MAC 帧格式。根据图 5.26所示的网络结构，用 802.11X 对双方身份进行认证并就双方采用的加密、解密算法及成对主密钥(PMK)达成共识的过程如图 5.27 所示。

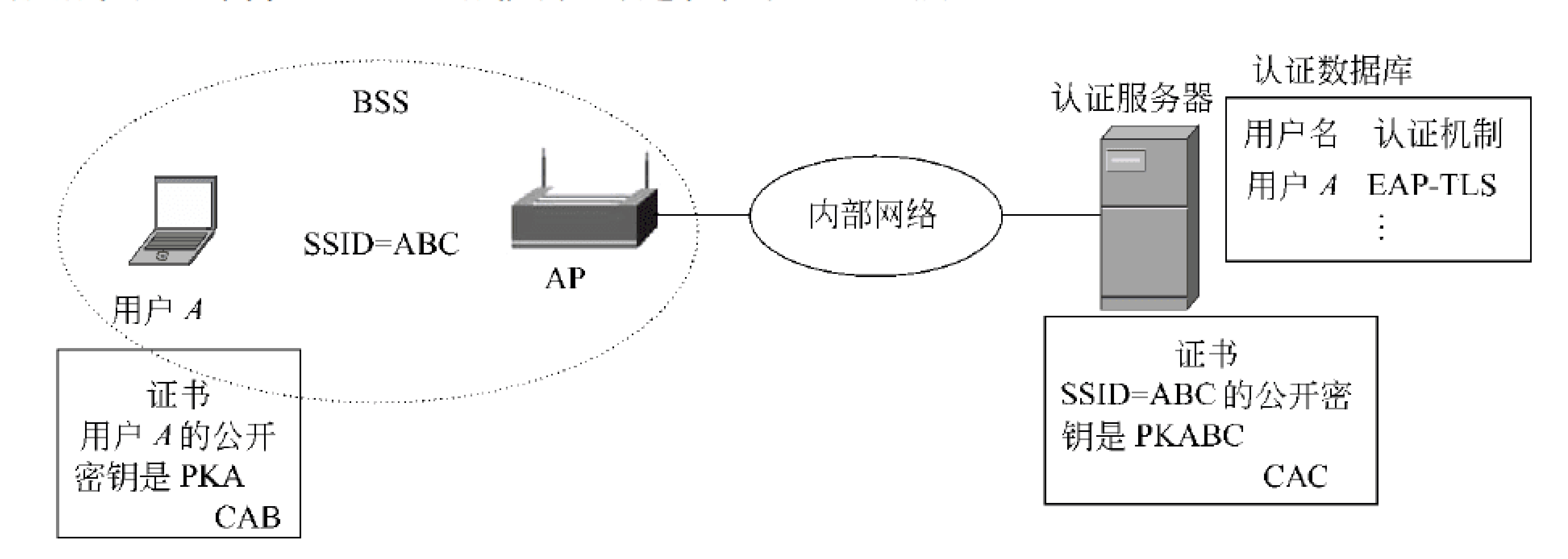


图 5.26 EAP-TLS 认证机制对应的网络结构

终端和 AP 之间完成图 5.23 所示的工作过程后，通过向 AP 发送 EAPOL-Start 帧开始双向认证过程，如图 5.27 所示。AP 接收到终端发送的 EAPOL-Start 后，通过 EAP 请求/响应过程要求终端提供用户名，并将包含用户名用户 *A* 的 EAP 响应报文封装成 RADIUS 请求接入报文传输给认证服务器。一般情况下，AP 和认证服务器之间用共享密钥加密相互间传输的 RADIUS 报文。认证服务器用用户名用户 *A* 检索认证数据库，找到匹配项，获知采用 EAP 为认证协议、TLS 为认证机制，因此，向终端发送一个启动 TLS 认证过程的 EAP 请求报文，当然，在认证服务器至 AP 的传输过程中，该 EAP 请求报文被封装成 RADIUS 的挑战接入报文。在 AP 至终端的传输过程中，该 EAP 请求报文又被封装成无线局域网的 MAC 帧。当终端接收到启动 TLS 认证过程的 EAP 请求报文，通过发送客户 Hello 消息开始 TLS 认证过程。客户 Hello 消息中给出用户 *A* 支持的

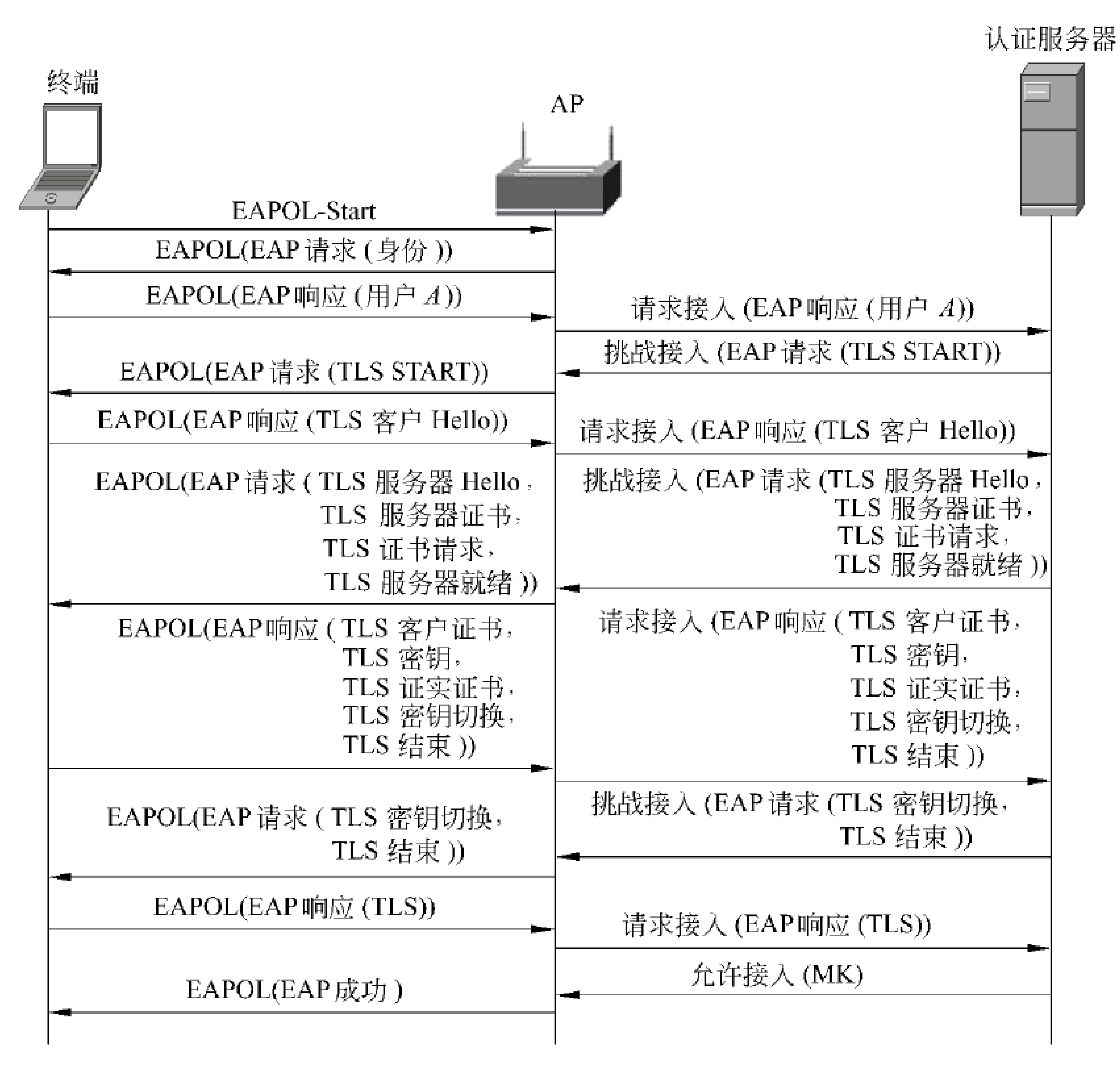


图5.27　EAP-TLS认证过程

加密解密算法列表、TLS版本号及终端生成的随机数RC等。客户Hello消息经AP转发后，到达认证服务器。认证服务器依次发送服务器Hello、服务器证书、证书请求及服务器就绪消息，这些消息封装在一个EAP请求报文中传输给终端。服务器Hello消息给出认证服务器在用户*A*支持的加密解密算法列表中挑选的加密解密算法，及认证服务器生成的随机数RS。服务器证书消息给出认证中心*C*为SSID＝ABC的BSS签发的证明BSS标识符(ABC)和公钥(PKABC)之间关联的证书，还包括有关能够让双方对认证中心的权威性达成共识的证明材料，即双方存在交集的证书链。由于需要双向认证，服务器通过证书请求消息要求终端发送证书，同时在证书请求消息中向终端给出认证服务器的证书链，方便终端在提供证书的同时，提供有关能够证明认证中心的证明材料。如果用户*A*和认证服务器使用的认证中心结构如图5.28所示，认证服务器发送的证书链为*A*＜＜*C*＞＞、*C*＜＜BSS＞＞。由于认证中心*A*是用户*A*和认证服务器各自证书链中的交集，用户*A*发送给认证服务器的证书链必须是*A*＜＜*B*＞＞、*B*＜＜用户*A*＞＞。终端接收到包含上述TLS消息的EAP请求报文后，首先根据证书链对认证服务器提供的证书进行鉴别。然后发送客户证书消息，其中包含的内容和服务器证书消息大致相同，给出由认证

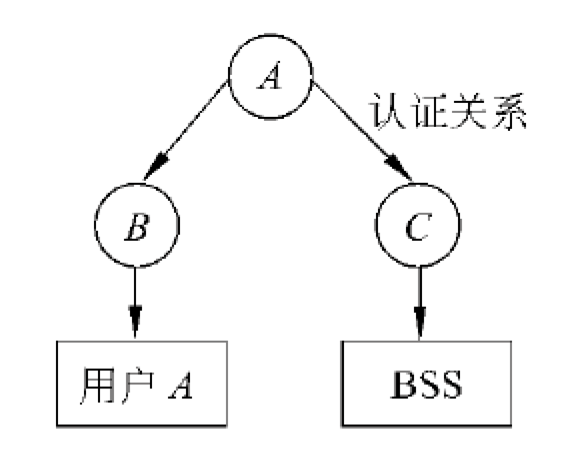


图5.28　认证中心结构

中心 B 签发的证明用户 A 和公钥 PKA 关联的证书。为了证实认证服务器的身份(拥有和 SSID=ABC 关联的公钥 PKABC 对应的私钥),向认证服务器发送密钥消息,密钥消息包含用和 SSID=ABC 关联的公钥 PKABC 加密预主密钥(PreMaster Secret,PMS)后产生的密文 Y_1($Y_1=E_{PKAS}$(PMS))。由于预主密钥(PMS)和用户 A、服务器生成的随机数(RC、RS)一起作为伪随机数生成器的随机数种子,用于生成主密钥(Master Secret,MS),因此,如果认证服务器不能解密出预主密钥,就无法通过伪随机数生成器产生主密钥,也就无法继续认证过程。但只要认证服务器能够解密出预主密钥,意味着认证服务器拥有和公钥 PKABC 对应的私钥,认证服务器的身份就得到证实。同样,终端只有证实自己拥有和证书中给出的公钥对应的私钥,才能证实自己的用户 A 身份,为此,向认证服务器发送证实证书消息,消息中给出用 PKA 对应的私钥 SKA 对双方发送的 TLS 消息进行报文摘要运算后得到的结果进行解密运算后产生的密文 Y_2($Y_2=D_{SKA}$(MD5(TLS 消息)))。如果认证服务器能够通过用和用户 A 关联的公钥 PKA 加密 Y_2 后,还原出 TLS 消息的报文摘要,可以确定发送者是用户 A。否则,终止认证过程。密钥切换消息表明终端开始使用预主密钥(PMS)和用户 A、服务器生成的随机数(RC、RS)为随机数种子,通过伪随机数生成器产生的主密钥。结束消息给出主密钥信息,用于双方通过求证主密钥来证实认证过程的完整性。结束消息包含的内容是用主密钥(MS)、MD(TLS 消息)为随机数种子,通过伪随机数生成器产生的随机数 Y_3($Y_3=$PRF(MS,"server finished",MD5(TLS 消息)‖SHA-1(TLS 消息)))。认证服务器接收到包含这些 TLS 消息的 EAP 响应报文后,认证终端身份,解密预主密钥(PMS),用 PMS、RC 和 RS 为随机数种子,通过伪随机数生成器产生主密钥(MS),向终端发送密钥切换消息和结束消息,结束消息包含的内容和终端发送的结束消息相同。终端接收到包含这些 TLS 消息的 EAP 请求报文,对认证服务器计算出的主密钥进行求证,如果和自己计算所得的主密钥相同,认证过程正常结束。否则,终止认证过程。在认证过程正常结束的情况下,终端已不需要再向认证服务器发送 TLS 消息,由于 EAP 协议规定必须对每一个请求报文作出响应,终端向认证服务器发送不包含任何 TLS 消息的空 EAP 响应报文。认证服务器接收到该 EAP 响应报文,向 AP 发送 RADIUS 允许接入报文,并在报文中给出由终端和认证服务器确定的主密钥(MS)。AP 随后向终端发送 EAP 成功报文,认证过程结束。主密钥 MS 作为用户 A 和 AP 之间的成对主密钥(PMK)用于密钥管理机制生成临时密钥 TK。

5.4.3 动态密钥分配机制

终端在认证过程中,不仅需要通过认证使得和 AP 之间的关联从非认证状态转变为认证状态,同时需要为经过该关联传输的数据分配临时密钥(Temporal Key,TK),之所以称为临时密钥是因为该密钥的使用寿命局限于这一次访问过程,当终端为下一次访问重新和 AP 建立关联时,将重新通过认证过程分配 TK。当终端和认证服务器完成双方认证后,AP 和终端具有相同的成对主密钥(PMK),终端和 AP 之间开始图 5.29 所示的密钥分配过程。终端接收到 AP 通过 EAPOL-KEY 帧传输的随机数 AN 后,根据 AP 生成的随机数 AN、自己生成的随机数 SN、成对主密钥(PMK)及双方的 MAC 地址,生成成对

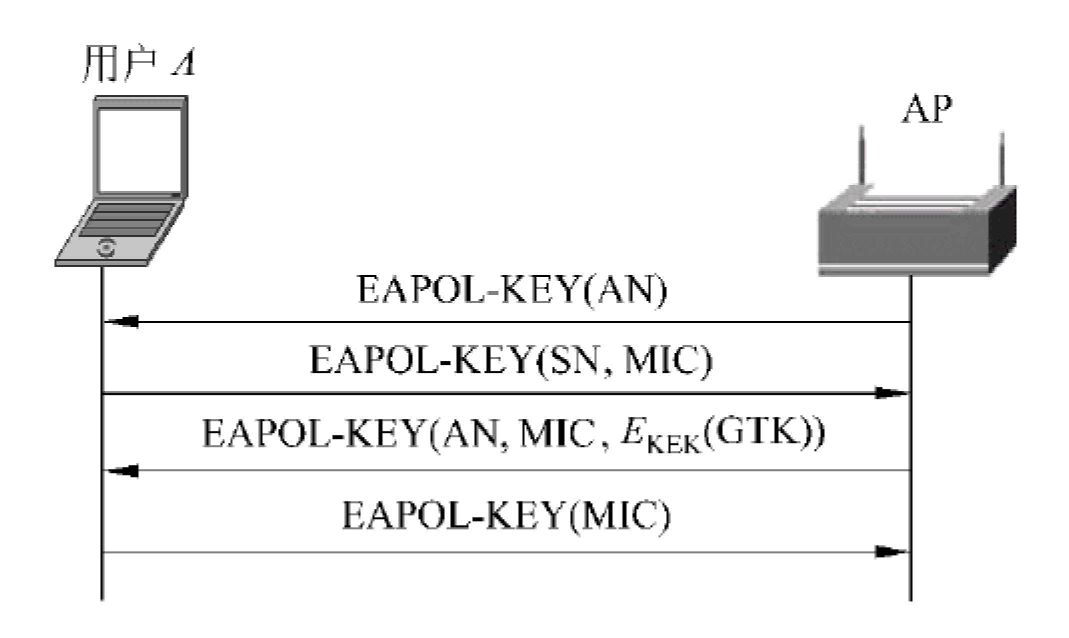


图 5.29　802.1X 密钥分配过程

过渡密钥(Pairwise Transient Key，PTK)。之所以称为成对过渡密钥，是因为该过渡密钥只用于和该关联相关的终端和 AP。TKIP 和 CCMP 生成的成对过渡密钥不同，由于 TKIP 用于数据加密和完整性检测的密钥不同(TK 和 MIC KEY)，而 CCMP 用同一个密钥进行数据加密和完整性检测，因此，TKIP 的成对过渡密钥(TKIP PTK)长度为512 位，而 CCMP 的成对过渡密钥(CCMP PTK)长度为 384 位。无论是 TKIP PTK，还是 CCMP PTK 都包含两个 802.11X 交换 EAPOL-KEY 帧需要的密钥：证实密钥(EAPOL-Key Confirmation Key，KCK)和加密密钥(EAPOL-Key Encryption Key，KEK)。KCK 用于对双方进行的密钥产生过程进行证实，KEK 用于加密密钥产生过程中传输的机密信息，TKIP PTK 包含用于加密这一次访问过程中终端和 AP 之间传输的数据的临时密钥 TK 和用于计算基于密钥的消息完整性编码(MIC)的 MIC 密钥，而 CCMP PTK 只包含用于加密数据和计算基于密钥的消息完整性编码(MIC)的临时密钥 TK，终端生成成对密钥的过程及 TKIP 和 CCMP 的密钥结构如图 5.30 所示。终端生成这些密钥后，通过 EAPOL-KEY 帧向 AP 发送随机数 SN，同时，用消息完整性编码(Message Integrity Code，MIC)证实终端密钥生成过程，MIC＝E_{KCK}(MD5(EAPOL-KEY 帧))。AP 获得终端的随机数 SN 后，同样根据图 5.30 所示的密钥生成过程产生这些密钥，根据接收到的 EAPOL-KEY 帧和生成的 KCK 重新计算出 MIC，将计算出的 MIC 和终端附在 EAPOL-

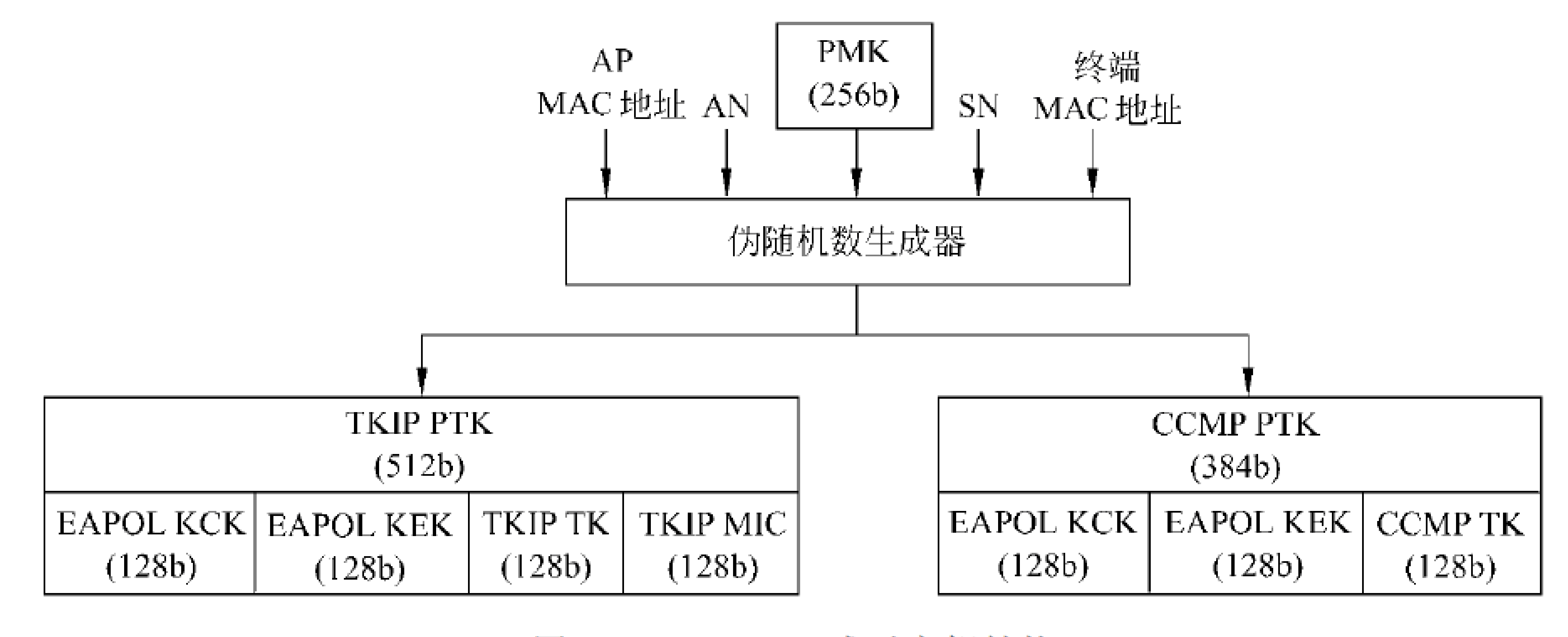


图 5.30　802.11i 成对密钥结构

KEY 帧后的 MIC 进行比较，如果相同，证明终端的密钥生成过程正确。AP 然后向终端发送 EAPOL-KEY 帧，一方面同样通过附在 EAPOL-KEY 帧后的 MIC 让终端证实 AP 的密钥生成过程，另一方面，向终端传输 AP 的临时广播密钥（Group Temporal Key，GTK），临时广播密钥用 KEK 加密，它的作用是加密 AP 向 BSS 中终端广播的数据，其生成过程如图 5.31 所示，AP 通过配置获得广播主密钥（GMK），GN 是 AP 选择的随机数。如果终端证实 AP 的密钥生成过程正确，通过向 AP 发送一个不含其他信息的空的 EAPOL-KEY 帧确认密钥分配过程结束。当然，空的 EAPOL-KEY 帧仍然用 MIC 让 AP 进行完整性检验。每当有终端和 AP 分离，AP 都需重新计算临时广播密钥 GTK，并将其传输给所有和其建立安全关联的终端，由于 AP 每一次计算 GTK 时选择不同的随机数 GN，因此，即使 GMK 不变，计算出的 GTK 也不同。

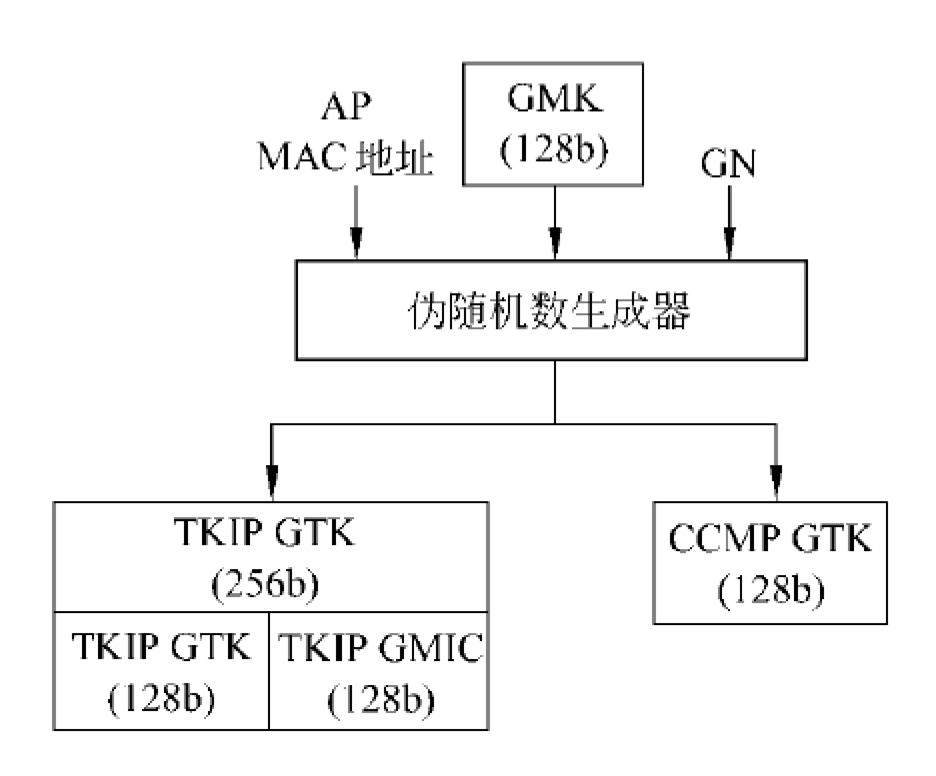


图 5.31 802.11i 组播密钥结构

习 题

5.1 无线局域网的安全性和以太网相比有什么不同？

5.2 检错和完整性检测有什么不同？为什么循环冗余检验码适合检错，但不适合数据完整性检测？

5.3 基于终端密钥分配机制和基于用户密钥分配机制有什么本质不同？

5.4 通过无线局域网传输数据一定要加密码？不加密有什么后果？

5.5 无线局域网和总线型以太网有什么本质区别？这种区别对安全性有什么要求？

5.6 WEP 如何加密数据和完整性检测？

5.7 如果图 5.32 中的无线局域网采用 WEP 安全机制，给出黑客终端非法访问内部网络服务器的全过程。

5.8 如果图 5.32 中无线局域网采用 802.11i 安全机制，给出用户终端接入无线局域网的全过程。

5.9 画出 TKIP 从数据到通过无线局域网传输的密文的全部封装过程。

5.10 画出 CCMP 从数据到通过无线局域网传输的密文的全部封装过程。

5.11 802.11i 如何实现基于用户分配密钥？

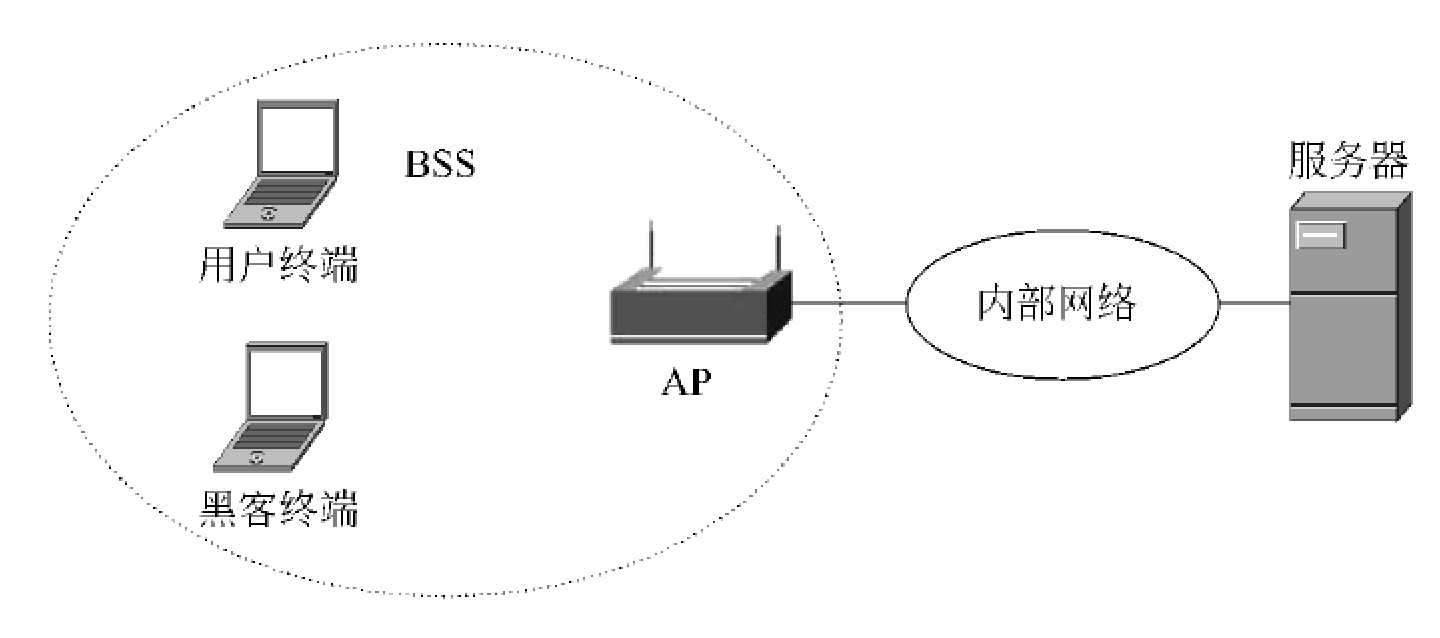


图 5.32　题 5.7 和题 5.8 图

5.12　解释 TKIP 加密和完整性检测机制优于 WEP 加密和完整性检测机制的理由？

5.13　解释 CCMP 加密和完整性检测机制优于 WEP 加密和完整性检测机制的理由？

5.14　802.11i 为什么用 TLS 作为认证机制？

5.15　无线局域网的安全关联和 IPSec 的安全关联有什么异同？

5.16　如果图 5.33 中所有接入网络的终端都需进行身份认证，给出和认证相关的所有配置？如果终端 A 允许漫游，既允许通过无线局域网接入，也允许通过以太网接入，如何解决终端 A 的配置？

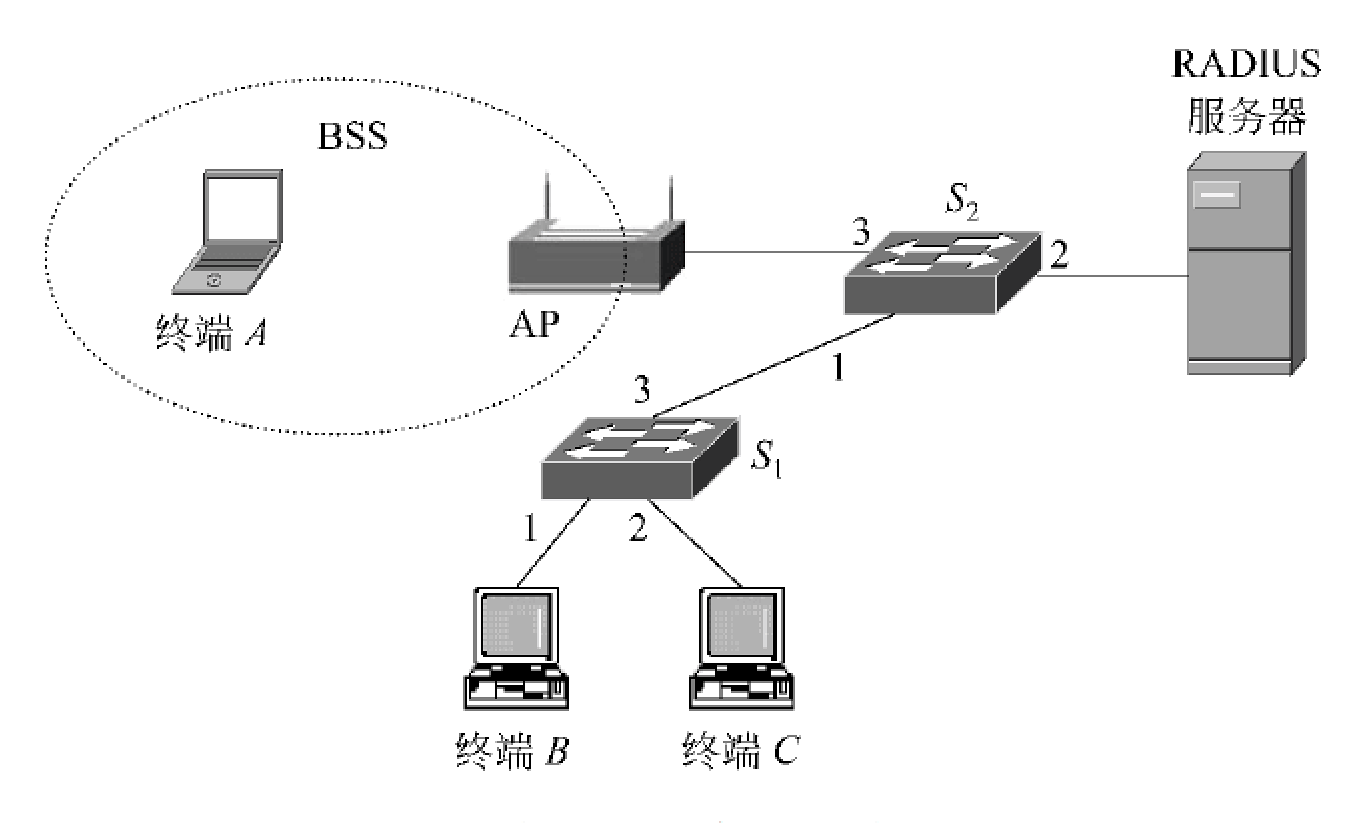


图 5.33　题 5.16 图

第 6 章 虚拟专用网络

CHAPTER

6.1 虚拟专用网络概述

专用网络是指网络基础设施和网络中的信息资源属于单个组织并由该组织对网络实施管理的网络结构，这种专用网络允许由分布在多个不同地区的子网互联而成，由于地区间相距甚远，子网间互联可以通过公共传输网络实现，但公共传输网络提供的必须是点对点的专用链路，且由专用网络独占点对点专用链路的带宽，以此保证专用网络由单个组织独占网络中的信息资源和通信资源的特性。图 6.1 就是一个专用网络结构，尽管各个子网间通过同步数字体系（Synchronous Digital Hierarchy，SDH）实现互联，但网络独占 SDH 提供的点对点专用链路的带宽。

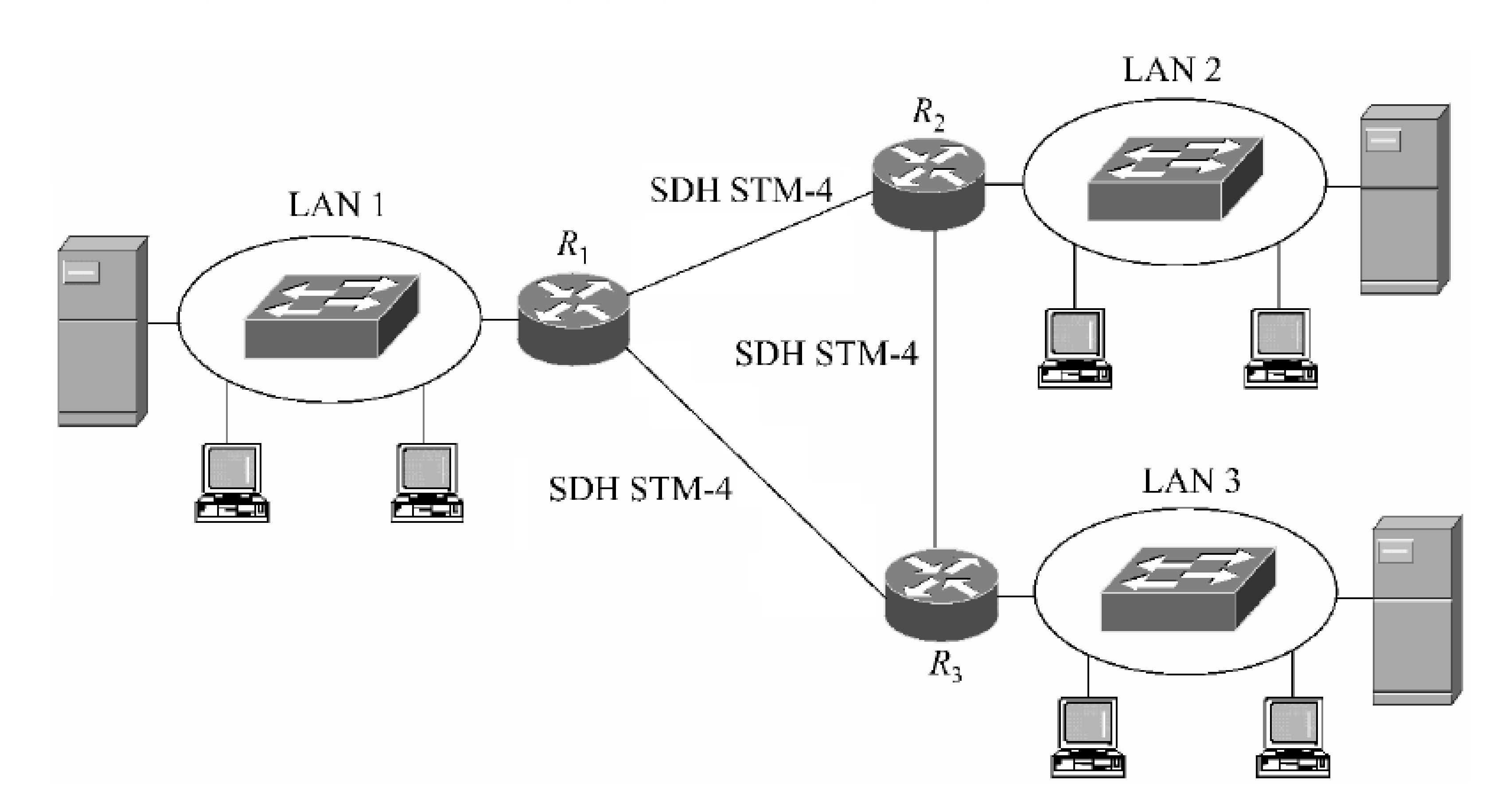


图 6.1 专用网络结构

图 6.1 所示的专用网络结构在实际操作过程中会出现一些问题，一是远距离 SDH 专用链路的租用费用极其昂贵。二是如果互连路由器的 SDH 专用链路的两端不属于同一个营运公司的话，如一端在上海，另一端在纽约，营运公司之间的协商过程是一个漫长、复杂的过程。三是由于子网间传输的数据的间歇性和突发性，点对点专用链路的利用率很低。为了

解决上述问题,可以改用数据交换网络实现子网间互联,图 6.2 就是通过 Internet 实现子网间互联的网络结构。

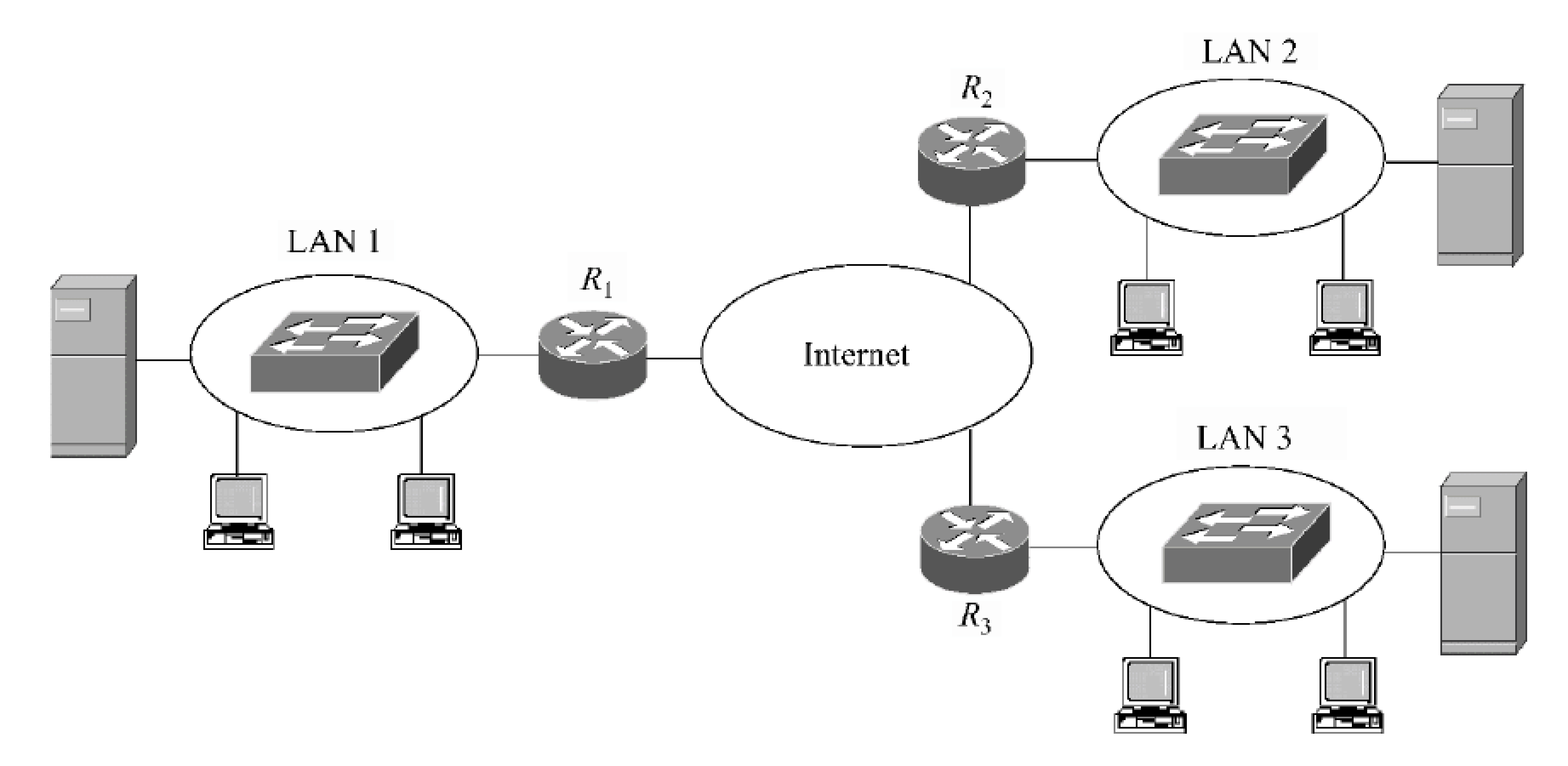


图 6.2 用 Internet 实现互联的网络结构

如果采用图 6.2 所示的网络结构,用点对点专用链路实现子网间互联的问题可以迎刃而解,由于 Internet 是全球最普及、最方便接入的网络,处于全球任何地区的子网均可很方便地接入 Internet,并通过 Internet 实现相互通信。由于 Internet 采用分组交换方式,通信费用比 SDH 的点对点专用链路便宜很多,而且,往往采用按流量计费,适合传输突发性、间歇性数据的应用环境。由于子网间传输路径的带宽是共享的,传输路径经过的分组交换结点属于公共传输网络的组成部分,随之而来的问题是子网间的带宽和数据传输安全无法得到保证,而这两点恰恰是构建专用网络的主要目的。很显然,需要一种既通过公共的分组交换网络,如 Internet,实现子网间互联,又使其具有专用点对点链路的带宽和传输安全保证的组网技术,这就是虚拟专用网络(Virtual Private Network,VPN)技术,加上虚拟就是表明用图 6.2 所示的网络结构实现图 6.1 所示网络结构具有的带宽和传输安全特性。

6.1.1 VPN 发展过程

1. 基于虚电路的 VPN 结构

在 Internet 十分普及之前,具有专用点对点链路的带宽和传输安全保证,又是采用分组交换网络,而不是电路交换网络作为互联网络的虚拟专用网络结构如图 6.3 所示,各个子网间用异步传输模式(Asynchronous Transfer Mode,ATM)或帧中继的虚电路(Virtual Circuit,VC)实现互联,VC 是链路层的点对点传输路径,多条 VC 可以复用同一条物理链路,因此,VC 采用帧交换(帧中继)或信元交换(ATM)技术,由于建立 VC 时为 VC 保留了一定的资源,如缓冲队列和输出链路带宽,而且,每一条 VC 是点对点专用的,不和其他用户共享,因此,无论是带宽和传输安全都有一定的保证。但一是目前 ATM 或帧中继的普及程度无法和 Internet 相比,使得图 6.3 中子网所在的区域有所限制。二是 VC 的通信费用比 Internet 的通信费用高出许多。三是由于帧或信元转发结点属于公共

传输网络的一部分，被所有用户共享，数据传输的安全性存在隐患。因此，随着 Internet 的普及，图 6.3 所示的虚拟专用网络结构逐渐不被人们所采用。

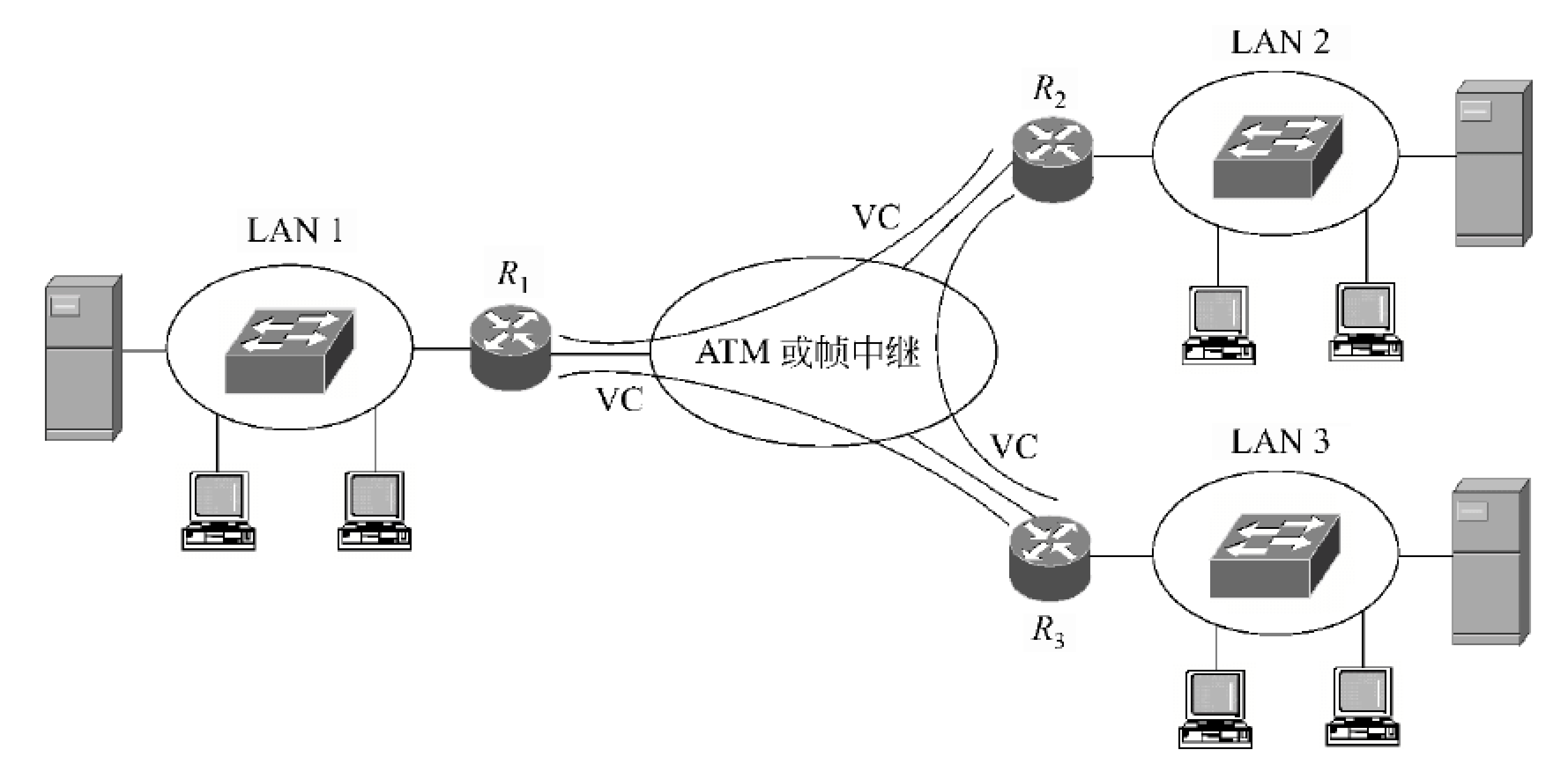


图 6.3　基于虚电路的 VPN 结构

2. 基于 IP 的 VPN 结构

在 Internet 十分普及之后，开始用 Internet 实现子网间互联，基于 IP 的 VPN 结构成为主流，为保证 VPN 各子网间传输路径的带宽和数据传输的安全性，在 IP 网络的基础上构建性能等同于点对点专用链路的隧道，并用隧道实现 VPN 各子网间的互联，根据隧道所传输的数据类型，将隧道分为 IP 隧道和第 2 层隧道，前者用于传输 IP 分组，后者用于传输链路层帧。

1）点对点 IP 隧道

隧道虽然通过公共区域，但它是封闭的，隧道内部和公共区域是相互隔绝的，IP 隧道的含义是虽然隧道两端之间的传输路径经过 IP 网络，但经过 IP 隧道传输的 IP 分组和其他经过 IP 网络传输的数据之间也是相互隔绝的，IP 隧道提供点对点专用链路的性能特性。用点对点 IP 隧道互联子网的 VPN 结构如图 6.4 所示。

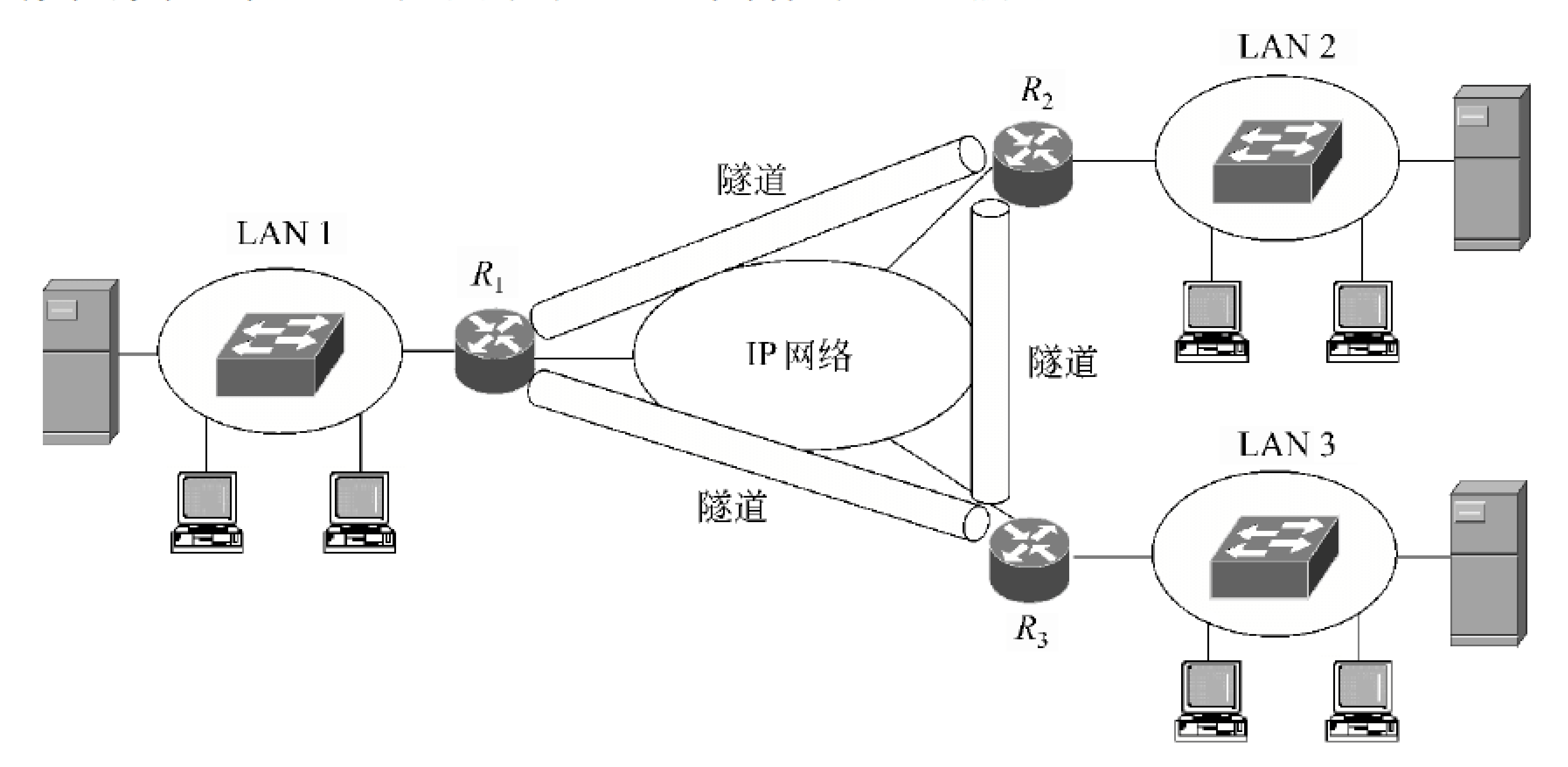


图 6.4　用 IP 隧道互联子网的 VPN 结构

2）虚拟接入网络

图 6.5 是远程用户终端拨号接入内部网络的过程，这种接入方式必须建立远程用户终端和内部网络中远程用户接入设备之间的点对点语音信道，当远程用户终端和内部网络相距甚远时，如内部网络位于北京，远程用户终端位于上海，维持远距离语音信道的费用非常昂贵，由于 PSTN 是电路交换网络，通过点对点语音信道这样的电路交换路径传输突发性、间歇性数据存在费用高、通信链路利用率低等诸多问题。

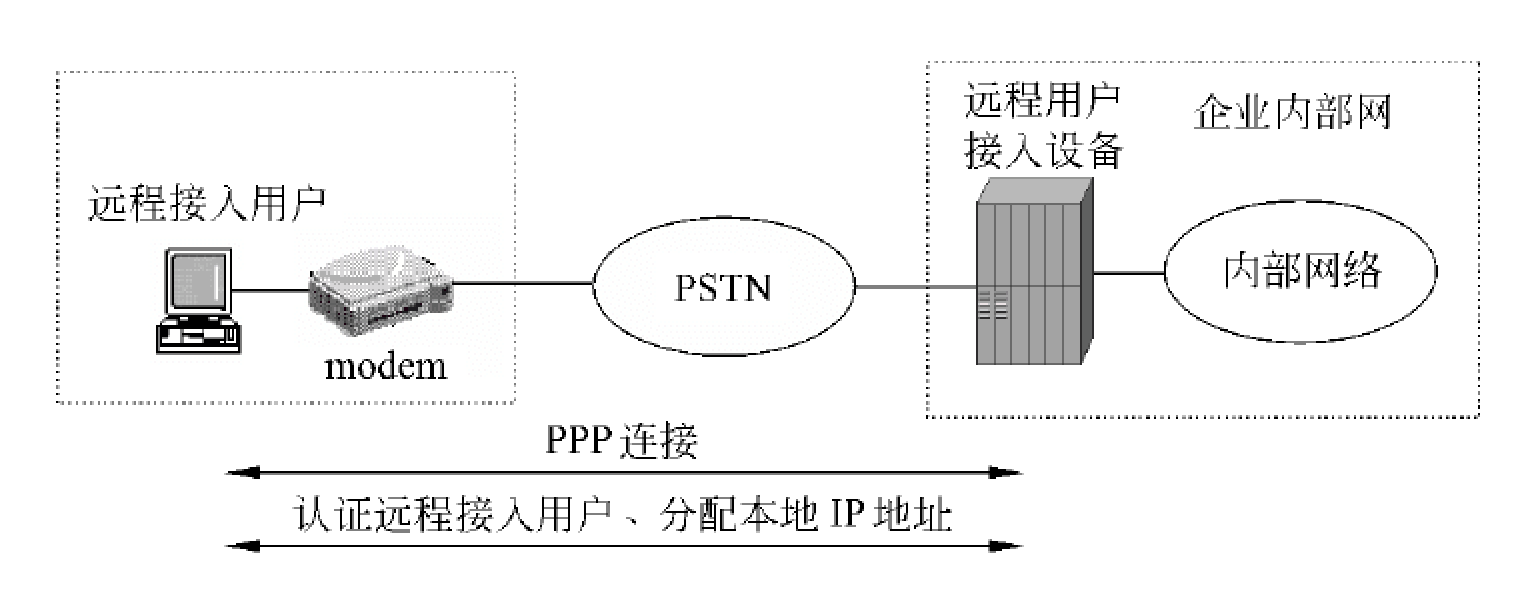


图 6.5 远程用户接入内部网络过程

图 6.6 和图 6.7 采用虚拟接入技术，它们和图 6.5 最大的不同在于将远程用户终端和内部网络之间的传输路径分成两部分，一部分是远程用户终端和本地服务提供者(Internet Service Provider，ISP)接入服务器之间建立的点对点语音信道，另一部分是本地 ISP 接入服务器和内部网络之间的分组交换路径，由于电路交换路径只存在于本地通信过程中，远距离通信过程由分组交换路径实现，因此，无论是端到端通信费用，还是通信链路的利用率都接近分组交换网络。图 6.6 和图 6.7 的不同在于第 2 层隧道的发起者，图 6.6 中，由用户终端发起建立第 2 层隧道，用户终端首先通过本地 ISP 接入 Internet，然后建立基于 Internet 的用户终端和内部网络之间的第 2 层隧道，对于用户终端和内部网络中的 L2TP 网络服务器(L2TP Network Server，LNS)，该第 2 层隧道等同于点对点专用链路，第 2 层隧道协议(Layer Two Tunneling Protocol，L2TP)用于建立、维持和删除第 2 层隧道，通过第 2 层隧道传输的是类似 PPP 帧和 MAC 帧这样的链路层帧。L2TP 网络服务器的功能类似于远程用户接入设备或网络接入服务器，只是

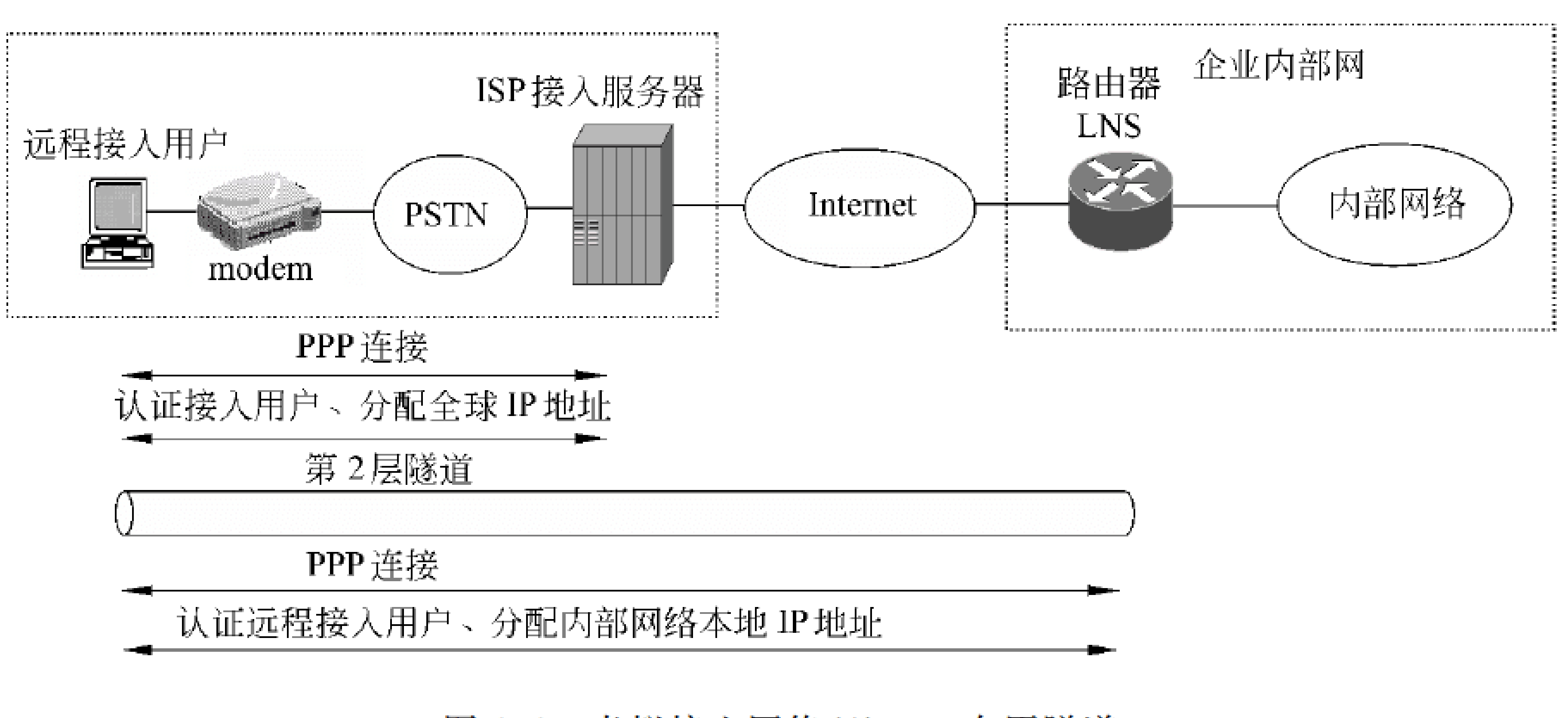


图 6.6 虚拟接入网络(1)——自愿隧道

L2TP 网络服务器是第 2 层隧道的端接设备,远程用户接入设备是语音信道的端接设备。图 6.7 中第 2 层隧道建立在 ISP 接入服务器和内部网络的 LNS 之间,由 ISP 接入服务器实现用户终端和 ISP 接入服务器之间语音信道和 ISP 接入服务器和内部网络 LNS 之间的第 2 层隧道之间的交接,这种既是第 2 层隧道的端接设备,又负责实现语音信道和第 2 层隧道之间交接的设备被称为 L2TP 接入集中器(Access Concentrator, LAC)。对于用户终端而言,由语音信道和第 2 层隧道组成的用户终端和内部网络 LNS 之间的传输路径完全等同于点对点专用链路,而内部网络的 LNS 也完全等同于远程用户接入设备。对于图 6.7 所示的虚拟接入网络,LAC 和 LNS 之间的第 2 层隧道由 ISP 接入服务器(LAC)发起建立,而触发 ISP 接入服务器发起建立第 2 层隧道过程的是 PSTN 的入呼叫信令。因此,图 6.7 中的第 2 层隧道是强制建立的,而图 6.6 中的第 2 层隧道是用户终端自愿发起建立的。

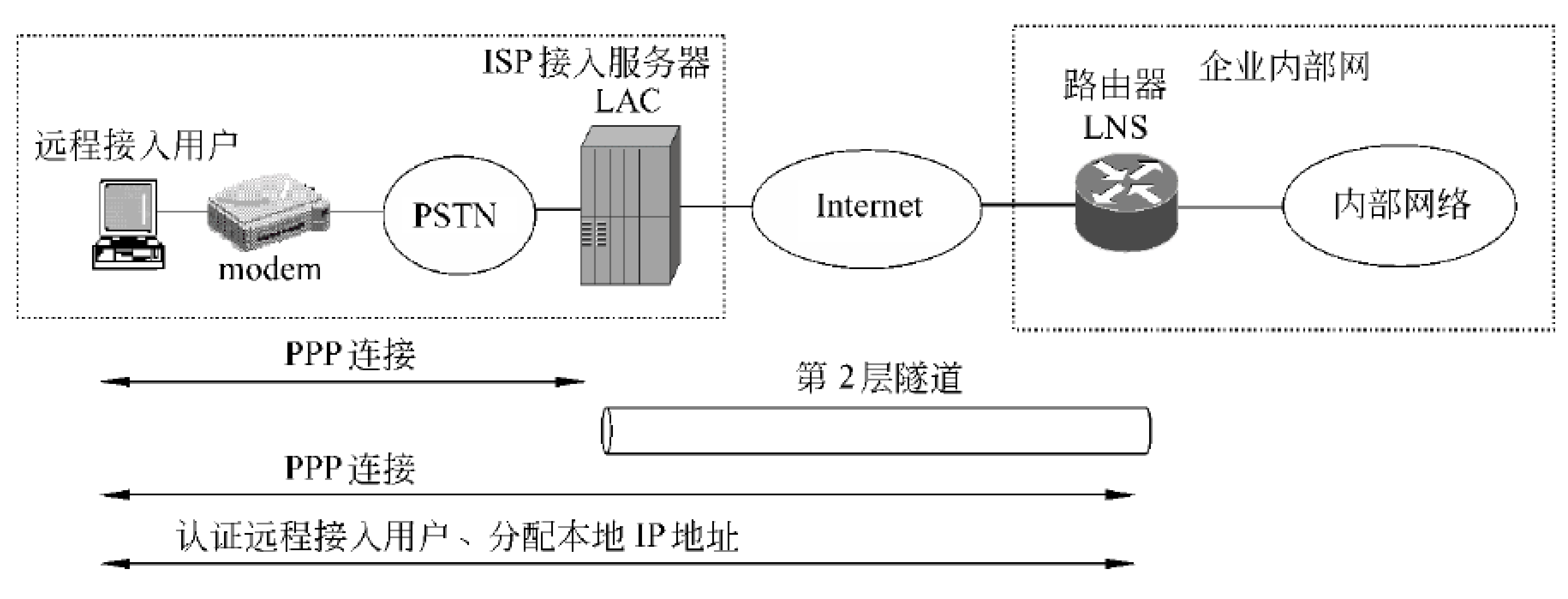


图 6.7　虚拟接入网络(2)——强制隧道

3) VPLS

虚拟专用局域网服务(Virtual Private LAN Service, VPLS)将多个相距甚远、用基于 IP 网络的第 2 层隧道连接的局域网作为单个局域网提供数据传输服务,图 6.8 是 VPLS 的网络拓扑结构,图 6.9 是图 6.8 对应的逻辑结构。

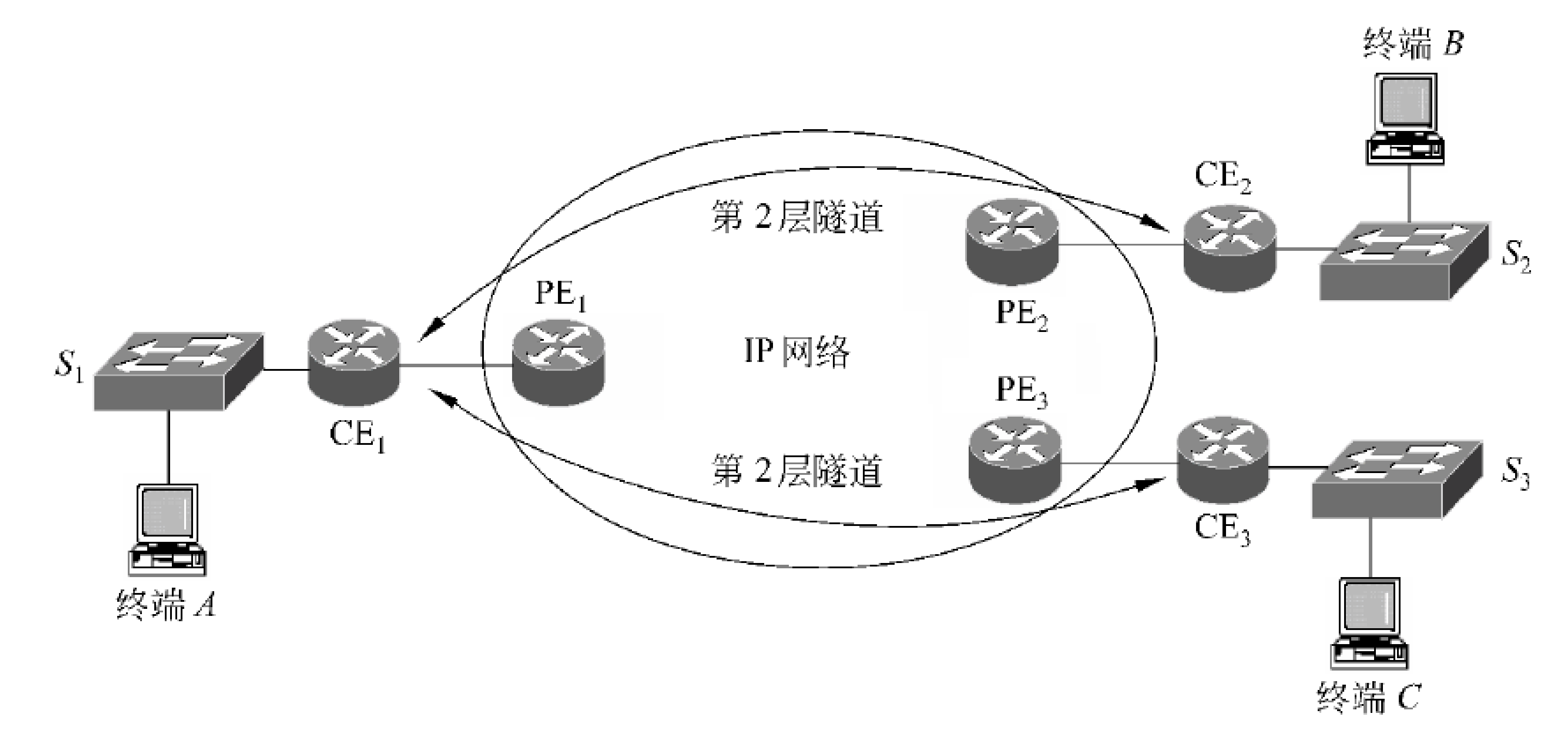


图 6.8　VPLS 网络拓扑结构

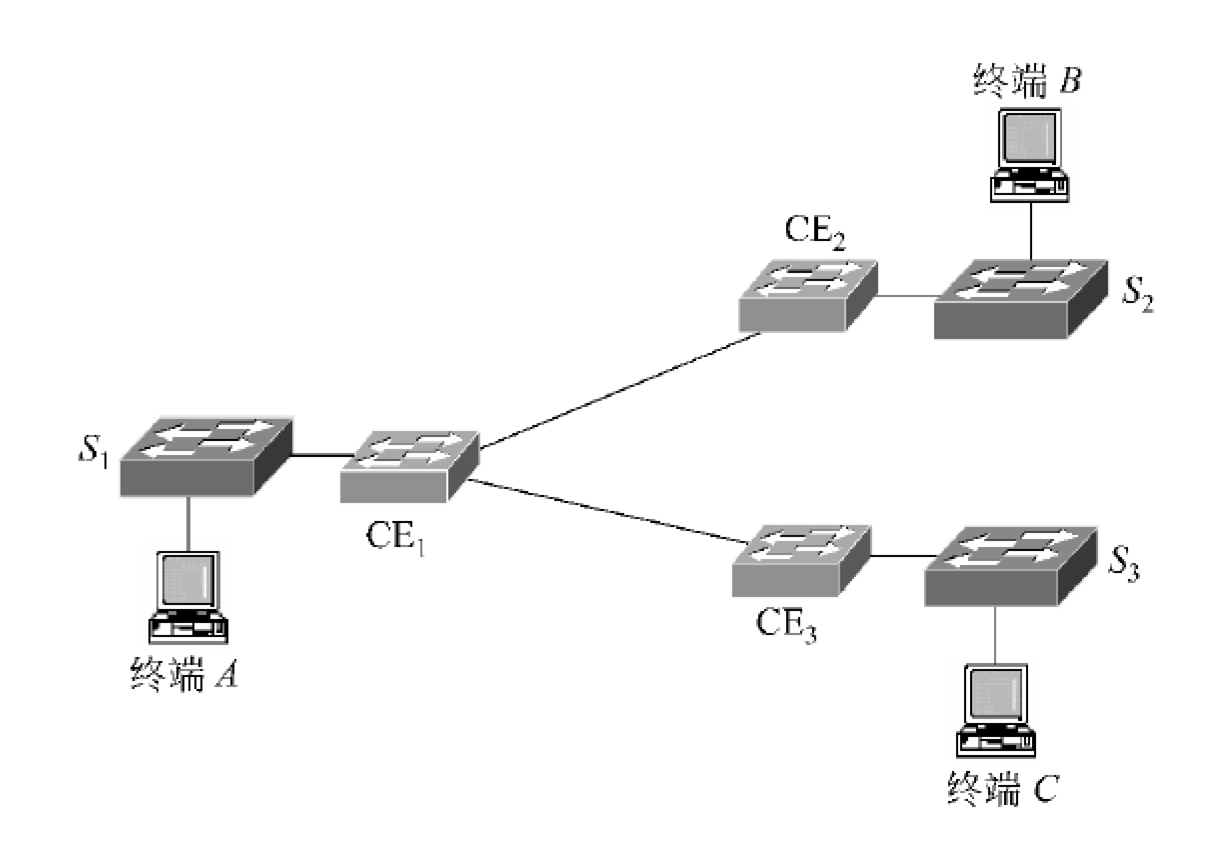


图 6.9 图 6.8 对应的逻辑结构

图 6.8 所示的网络结构中，用户边缘路由器(Customers' Edge router，CE)对于局域网而言，是桥设备，由它实现地址学习、站表维护和 MAC 帧转发功能，在实现上述功能过程中，基于 IP 网络的第 2 层隧道等同于互连交换机的物理链路，因此，被称为虚拟线路(PseudoWire，PW)，每一条第 2 层隧道和以太网端口一样参与地址学习、站表维护和 MAC 帧转发过程。对于 IP 网络而言，CE 是边缘路由器，将封装成 IP 分组格式的第 2 层隧道报文传输给 IP 网络中的提供者边缘路由器(Service Provider's Edge router，PE)，并经过 IP 网络到达第 2 层隧道另一端的 CE。

3. 基于 MPLS 的 VPN 结构

1) 基于 MPLS 的第 2 层 VPN 结构

多协议标签交换(MultiProtocol Label Switching，MPLS)网络在 PE 之间建立标签交换路径(Label Switched Path，LSP)，LSP 等同于单向的点对点链路，在图 6.10 所示的基于 MPLS 的第 2 层 VPN 结构中，PE 一方面作为 MPLS 网络的边缘路由器，参与 PE 之间 LSP 的建立，另一方面，PE 对于内部网络又是一个桥设备，实现连接 LAN 路由器 $R_i(i=1,2,3)$的 VC 和 PE 之间 LSP 的交接，并完成 VC 对应的数据封装格式和 MPLS 帧封装格式之间的相互转换。因此，对于 LAN 路由器而言，图 6.10 所示的网络结构的功能完全等同于图 6.11 所示的逻辑结构。

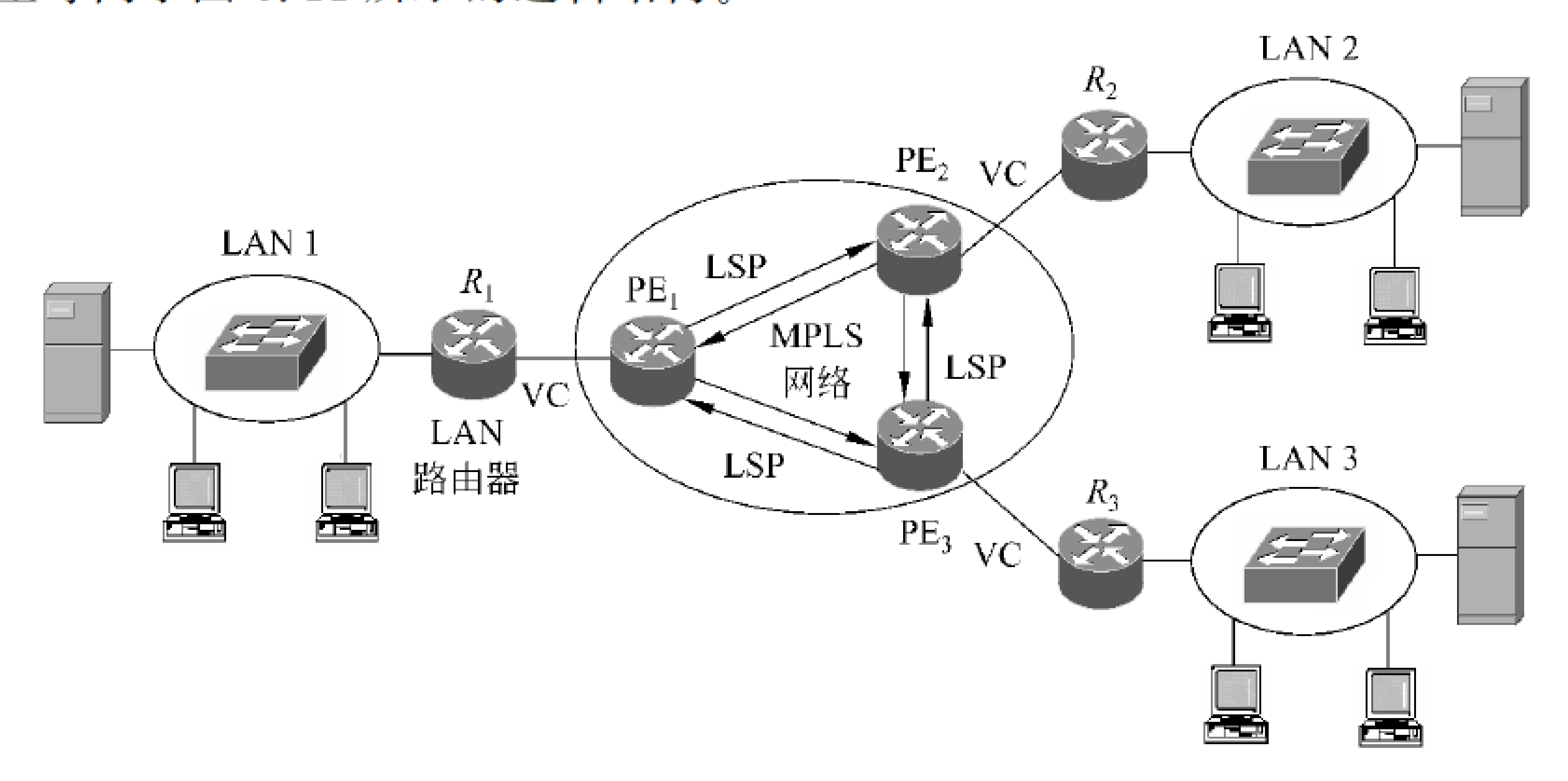


图 6.10 基于 MPLS 的第 2 层 VPN 结构

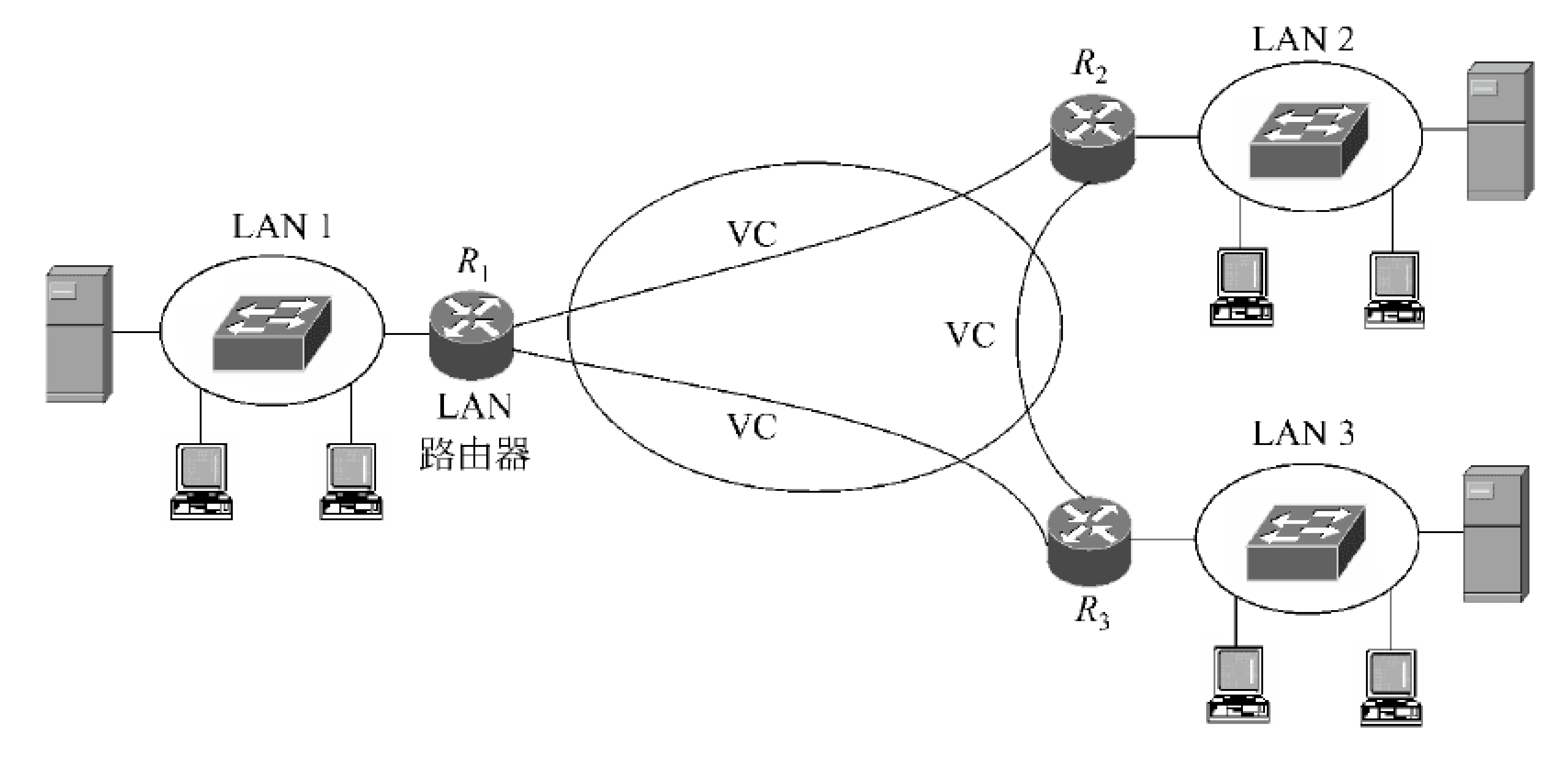


图 6.11　图 6.10 对应的逻辑结构

2）基于 MPLS 的第 3 层 VPN 结构

如果 PE 对于内部网络是路由器设备，图 6.10 所示的网络结构就是基于 MPLS 的第 3 层VPN 结构，LSP 就是 PE 之间的单向点对点链路，PE 一方面作为 MPLS 网络的边缘路由器，参与 PE 之间 LSP 的建立，另一方面作为内部网络的路由器参与路由内部网络各个子网间传输的 IP 分组。

4. 各种 VPN 结构的比较

随着 Internet 的发展和普及，基于 IP 网络的 VPN 结构逐渐成为主流技术，基于 VC 的 VPN 结构逐渐被淘汰出局，随着 MPLS 网络的兴起，和 LSP 交换转发的特性，基于 MPLS 的 VPN 结构逐渐成为 VPN 的首选技术。MPLS 网络是 IP 路由技术和 VC 交换技术的完美结合，因此，也是 Internet 发展和普及的产物。由于基于 IP 网络的 VPN 结构能够和 IPSec 完美结合，它的安全性优于基于 MPLS 的 VPN 结构，因此，如果单纯从网络安全性出发，基于 IP 网络的 VPN 结构是最佳选择，这也是本章重点讨论基于 IP 网络的 VPN 结构的原因。

6.1.2　VPN 安全机制

可以通过图 6.12 所示的汽车从巴黎经过英吉利隧道到伦敦的例子来说明一下隧道传输数据的过程，当汽车经过英吉利隧道时，不能直接驶过隧道，而是需要被装载到高速列车上，通过高速列车将其从隧道的一端传输到隧道的另一端。因此，汽车在隧道的入口被装载到高速列车上，在隧道的出口被重新下载到公路上。当链路层帧或 IP 分组经过隧道传输时，也不能直接以链路层帧或 IP 分组的封装格式在隧道内传输，而是必须在隧道的入口封装成隧道所要求的格式，在隧道的出口被重新还原成原来的封装格式。隧道封装格式解决数据经过隧道传输的问题，但不能解决数据经过隧道传输所引发的安全问题，在基于 IP 网络的 VPN 结构中，隧道是经过 IP 网络的端到端传输路径，隧道封装格式只能解决数据经过 IP 网络的端到端传输过程，但无法解决数据经过 IP 网络传输所引发的安全问题，经过 IP 网络安全传输数据的机制是加密、认证和完整性检测，加密保证数据经过 IP 网络传输时不被窃取，完整性检测能够检测出数据在传输过程中是否被篡改，认证

保证数据在隧道两端之间传输，这些安全功能恰恰是 IPSec 的功能，而不是隧道的功能，为了将隧道和 IPSec 完美结合，必须在经过隧道传输数据前，在隧道两端建立双向的安全关联，并对经过隧道传输的数据进行加密、认证和完整性检测。

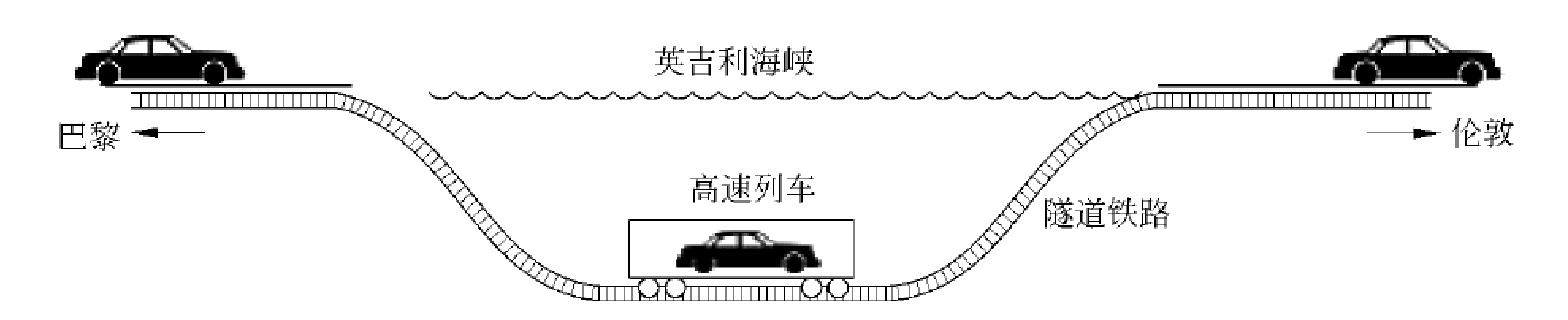


图 6.12　汽车经过英吉利隧道的过程

6.2　点对点 IP 隧道

6.2.1　网络结构

图 6.13 是采用基于 IP 网络 VPN 技术的企业内部网络结构，企业内部网络中的各个子网采用本地 IP 地址，如 LAN 1 的子网地址 193.1.1.0/24，LAN 2 的子网地址 193.1.2.0/24 和LAN 3 的子网地址 193.1.3.0/24。各个子网虽然分布在各地，通过 Internet 实现互联，但不同子网内终端之间通信仍然使用本地 IP 地址，而不是全球 IP 地址。企业内部网络中路由器 R_1、R_2 和 R_3 连接 Internet 的端口需要分配全球 IP 地址，如路由器 R_1 端口 2 分配的 IP 地址 200.1.1.1，路由器 R_2 端口 2 分配的 IP 地址 200.1.2.1 和路由器 R_3 端口 2 分配的 IP 地址 200.1.3.1，而且这些端口作为互联内部网络路由器的点对点 IP 隧道的两端，由于这些隧道用来传输 IP 分组，因此，被称为三层隧道，它们等同于点对点链路。

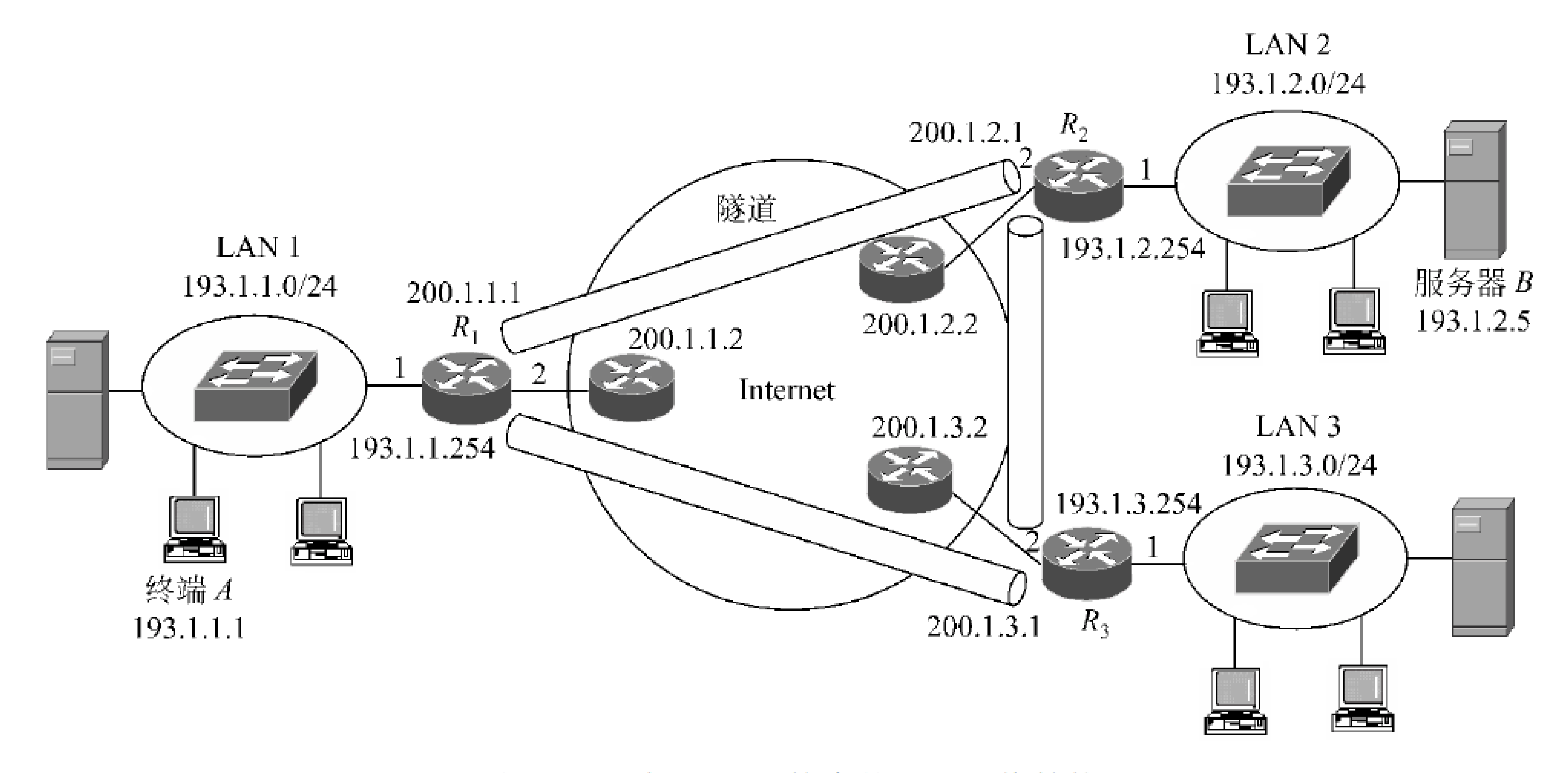


图 6.13　采用 VPN 技术的企业网络结构

图6.13所示的VPN需要实现两部分功能：一是需要实现子网之间使用本地IP地址的IP分组的相互交换。二是需要实现隧道的封闭性、安全性，使外部用户无法窃取和篡改经过隧道传输的数据。

6.2.2　IP分组传输机制

为了通过路由器R_1、R_2和R_3实现使用本地IP地址的IP分组的跨子网传输，首先必须在路由器R_1定义两条隧道：

隧道1：200.1.1.1　200.1.2.1

隧道2：200.1.1.1　200.1.3.1

定义隧道只需给出隧道两端的全球IP地址，在定义完隧道后，必须定义路由表，路由器R_1的路由表如表6.1所示。

表6.1　路由器R_1路由表

目的IP地址	子网掩码	转发端口	下一跳路由器
193.1.1.0	255.255.255.0	1	直接
193.1.2.0	255.255.255.0	隧道1	—
193.1.3.0	255.255.255.0	隧道2	—
200.1.2.1	255.255.255.255	2	200.1.1.2
200.1.3.1	255.255.255.255	2	200.1.1.2

路由器R_2定义下述两条隧道及表6.2所示的路由表。

隧道1：200.1.2.1　200.1.1.1

隧道2：200.1.2.1　200.1.3.1

表6.2　路由器R_2路由表

目的IP地址	子网掩码	转发端口	下一跳路由器
193.1.1.0	255.255.255.0	隧道1	—
193.1.2.0	255.255.255.0	1	直接
193.1.3.0	255.255.255.0	隧道2	—
200.1.1.1	255.255.255.255	2	200.1.2.2
200.1.3.1	255.255.255.255	2	200.1.2.2

路由器R_3定义下述两条隧道及表6.3所示的路由表。

隧道1：200.1.3.1　200.1.1.1

隧道2：200.1.3.1　200.1.2.1

表 6.3 路由器 R_3 路由表

目的 IP 地址	子网掩码	转发端口	下一跳路由器
193.1.1.0	255.255.255.0	隧道 1	—
193.1.2.0	255.255.255.0	隧道 2	—
193.1.3.0	255.255.255.0	1	直接
200.1.1.1	255.255.255.255	2	200.1.3.2
200.1.2.1	255.255.255.255	2	200.1.3.2

在完成 R_1、R_2、R_3 的路由表的配置后，就可在子网之间相互交换使用本地 IP 地址的 IP 分组，假定子网 1 内 IP 地址为 193.1.1.1 的终端 A，希望访问子网 2 中 IP 地址为 193.1.2.5 的服务器 B，它构建以 193.1.1.1 为源 IP 地址，以 193.1.2.5 为目的 IP 地址的 IP 分组，由于终端 A 的默认网关为 193.1.1.254，终端 A 将该 IP 分组发送给路由器 R_1。路由器 R_1 接收到该 IP 分组后，用该 IP 分组的目的 IP 地址去查找路由表，找到匹配项：193.1.2.0/24 隧道 1，通过隧道 1 的定义知道隧道两端的全球 IP 地址，将该 IP 分组封装成隧道格式。隧道格式实际上就在该 IP 分组外部再加上一个 IP 首部，外层 IP 首部的源 IP 地址为 200.1.1.1，目的 IP 地址为 200.1.2.1，即隧道两端的全球 IP 地址，隧道格式如图 6.14 所示。



图 6.14 封装成隧道格式过程

隧道格式也是一个 IP 分组，只是它的数据字段包含了另一个 IP 分组，就像在一封信件外面套上另一个信封，并重新写上寄信人、收信人地址。

路由器 R_1 同样通过查找路由表，将隧道格式的 IP 分组转发给 Internet 中的下一跳路由器，并经过 Internet 到达路由器 R_2。路由器 R_2 通过检查隧道格式的 IP 分组的协议类型字段，获知它是隧道格式，数据字段中封装了另一个 IP 分组。将另一个 IP 分组从隧道格式的数据字段中分离出来，再以该 IP 分组的目的 IP 地址去查找路由表，找到匹配项：193.1.2.0/24 端口 1 直接，将该 IP 分组通过端口 1 连接的以太网转发出去，最终到达 IP 地址为 193.1.2.5 的服务器。当然，从端口 1 转发出去的 IP 分组必须先封装成 MAC 帧，并以路由器 R_2 端口 1 的 MAC 地址为该 MAC 帧的源 MAC 地址，服务器 B 网卡的 MAC 地址为该 MAC 帧的目的 MAC 地址。如果路由器 R_2 事先不知道服务器 B 网卡的 MAC 地址，需先根据服务器 B 的 IP 地址，通过 ARP 获得服务器 B 网卡的 MAC 地址。

6.2.3 安全机制

1. 建立 IPSec 安全关联

隧道技术只能解决通过隧道传输无法直接在隧道所经过的公共分组交换网络传输的数据封装格式,但无法解决经过公共分组交换网络传输的数据的安全性问题。如图 6.13 所示的 VPN 结构中,由于企业内部网络中的各子网采用本地 IP 地址,而 Internet 无法路由以本地 IP 地址为源和目的 IP 地址的 IP 分组,因此,LAN 1 中终端 A 发送给 LAN 2 中服务器 B 的以 193.1.1.1 为源 IP 地址,193.1.2.5 为目的 IP 地址的 IP 分组无法直接在 Internet 上传输,一旦封装成隧道格式后,由于隧道格式的 IP 分组的外层 IP 首部中的源和目的 IP 地址(200.1.1.1 和 200.1.2.1)为 Internet 全球 IP 地址,因此,能够经过 Internet 实现从路由器 R_1 端口 2 到路由器 R_2 端口 2 的传输过程,但无法保证隧道格式中内层 IP 分组的保密性和完整性。用于保证隧道格式中内层 IP 分组经过 Internet 传输时的保密性和完整性的机制是 IPSec 的隧道模式,对于 LAN 1 中终端 A 至 LAN 2 中服务器 B 的传输过程,它首先需要建立路由器 R_1 端口 2 至路由器 R_2 端口 2 的安全关联,建立安全关联的过程就是隧道两端协商安全参数的过程,因此,必须配置相关安全参数并与隧道绑定在一起。路由器 R_1 端口 2 和路由器 R_2 端口 2 需要配置相同的安全参数,假定配置的安全参数如下所示。

- 安全协议:ESP。
- 加密算法:AES。
- D-H 组号:2。
- 认证算法:HMAC-MD5-96。
- 模式:隧道。

安全关联可以静态配置,也可以由 Internet 安全关联和密钥管理协议(Internet Security Association and key Management Protocol,ISAMP)动态建立,如果由 ISAMP 动态建立安全关联,必须由 ISAMP 完成隧道两端身份认证、密钥分配和安全参数协商过程,由于密钥分配和安全参数协商过程中需要在隧道两端相互传输一些敏感数据,因此,需要保证这些敏感数据经过 Internet 传输时的保密性和完整性,为此,ISAMP 将安全关联建立过程分为两个阶段,第 1 阶段用于建立安全传输敏感数据的传输通道,第 2 阶段实现密钥分配和安全参数协商过程。其实这两个阶段实现的功能是相似的,只是对象不同,第 1 阶段建立安全传输通道的目的是为了保证密钥分配和安全参数协商过程中传输的数据的安全性和完整性,第 2 阶段建立安全关联的目的是保证企业内部网络中各子网间经过 Internet 传输的数据的保密性和完整性。为了建立安全传输敏感数据的传输通道,同样需要在隧道两端配置相关参数。

- 加密算法:DES。
- D-H 组号:2。
- 认证机制:数字签名。
- 完整性检测算法:数字签名。

采用数字签名认证机制和完整性检测的过程如图 6.15 所示,隧道两端路由器首先通

过向认证中心注册，获得公钥和私钥对，路由器 R_1 为 PKR1 和 SKR1，路由器 R_2 为 PKR2 和 SKR2，并在认证中心证书库中生成证明路由器名和公钥之间关联的证书。在开始认证过程前，隧道两端路由器通过访问认证中心证书库获得对方的证书，并因此获得对方的公钥，当路由器 R_1 向路由器 R_2 发送数据 P 时，根据报文摘要算法计算出数据的报文摘要 MD(P)(MD 为报文摘要算法，可以是 MD5 或 SHA-1)，然后用自己的私密对报文摘要进行解密运算 D_{SKR1}(MD(P))，将 D_{SKR1}(MD(P))作为数字签名附在数据后面一起发送给路由器 R_2，路由器 R_2 根据相同的报文摘要算法计算出数据 P 的报文摘要 MD(P)，用路由器 R_1 的公钥对附在数据后的数字签名进行加密运算 E_{PKR1}(D_{SKR1}(MD(P)))=MD(P)，然后将两者进行比较，如果相等，表示数据确实由路由器 R_1 发送且传输过程中未被篡改，否则，表示认证和完整性检测失败。

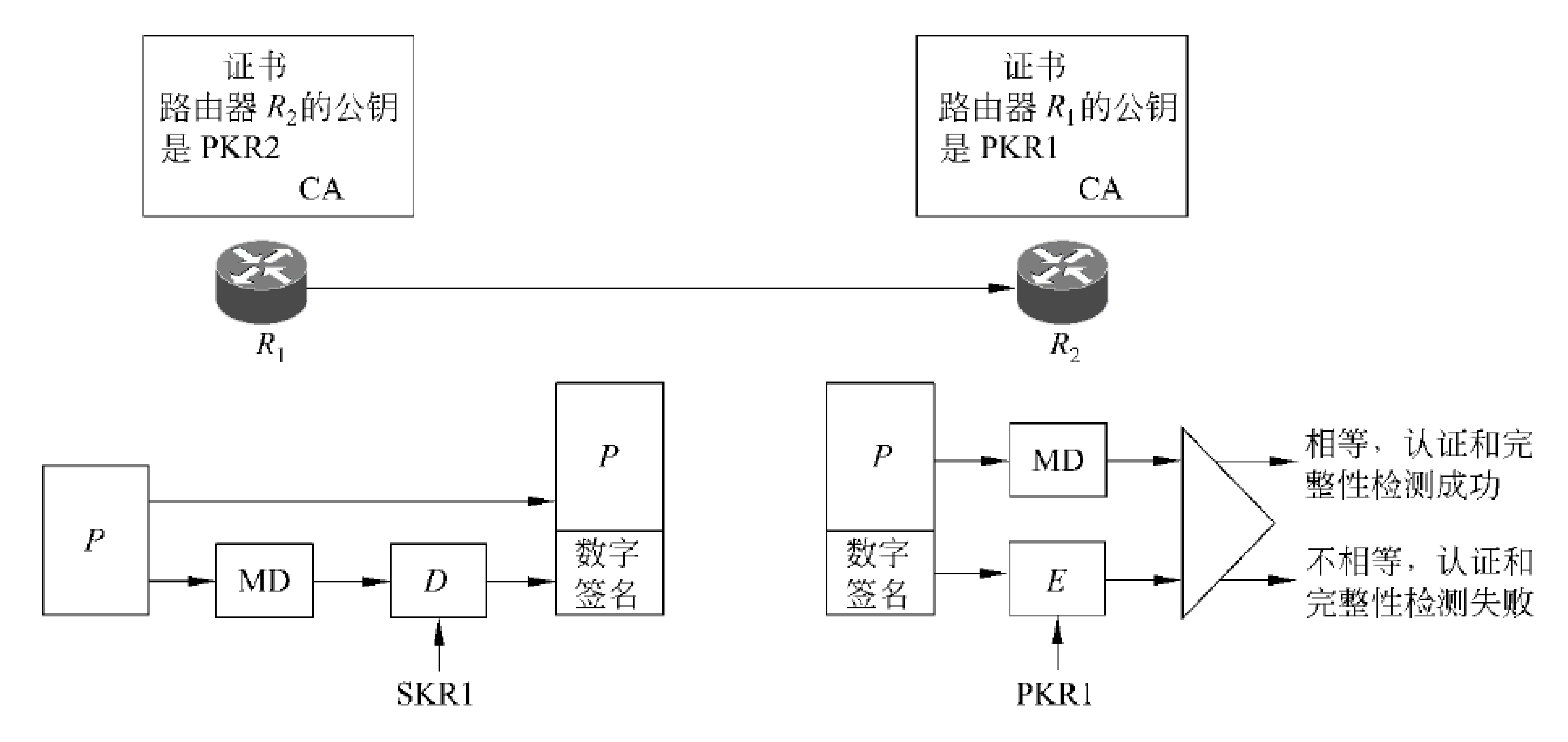


图 6.15 认证和完整性检测过程

隧道两端路由器建立安全传输敏感数据的传输通道的过程实际上也是协商加密、认证算法，分配密钥的过程，如图 6.16 所示。路由器 R_1 向路由器 R_2 发送为安全传输通道配置的安全算法，如加密算法(DES)、密钥分配协议(D-H-2)、认证和完整性检测算法(数字签名)等，路由器 R_1 发送的可以是它所支持的安全算法列表，路由器 R_2 在路由器 R_1 支持的安全算法列表中选择它所支持的安全算法，并向路由器 R_1 回送该组安全算法。路由器 R_1 接收到路由器 R_2 支持的安全算法后，选择该组安全算法作为安全传输通道所使用的安全算法，如本例中双方选择：

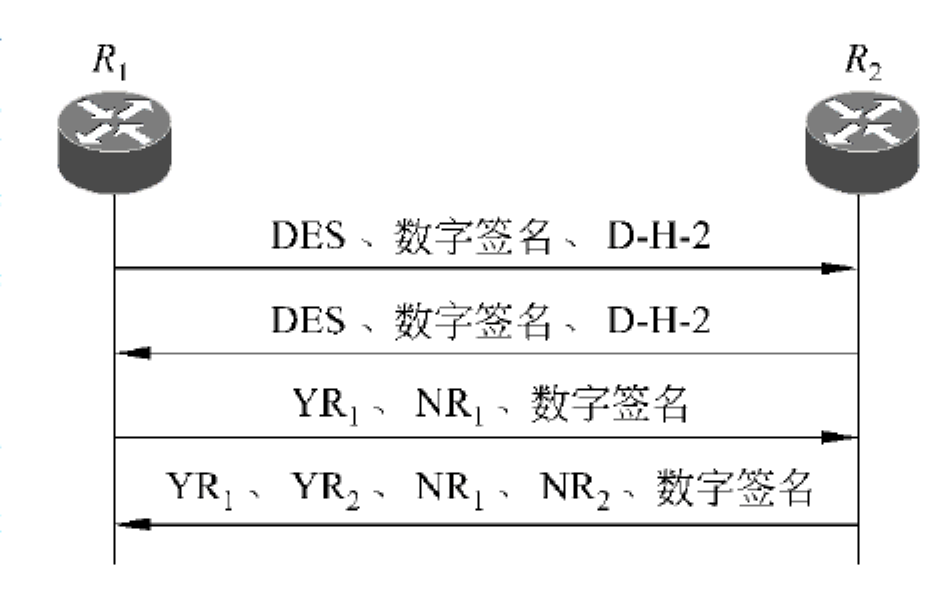


图 6.16 建立安全传输通道的过程

- 加密算法 DES。
- 认证和完整性检测算法 数字签名。
- 密钥分配协议 D-H-2。

密钥分配协议 D-H-2 是指采用 Diffie-Hellman 密钥交换算法，第 2 组大素数 q 和原

根 α 值，双方通过交换公钥 YR_1 和 YR_2 分配密钥（密钥 $K=YR_2^{XR_1} \bmod q=YR_1^{XR_2} \bmod q$），为了防中继攻击（亦称重放攻击），交换公钥时，携带随机数 NR_1 和 NR_2，同时，对公钥（YR_1 和 YR_2）和随机数（NR_1 和 NR_2）进行数字签名，路由器 R_1 发送给路由器 R_2 的公钥和随机数的数字签名是 $D_{SKR1}(MD(YR_1 \| NR_1))$，路由器 R_2 发送给路由器 R_1 的公钥和随机数的数字签名是 $D_{SKR2}(MD(YR_1 \| YR_2 \| NR_1 \| NR_2))$，这样接收端可以通过携带的数字签名认证发送端并进行数据的完整性检测。

建立安全传输通道后，可以交换建立安全关联所需要的数据，在交换建立安全关联所需要的数据时，可以用密钥 $K=YR_2^{XR_1} \bmod q=YR_1^{XR_2} \bmod q$ 和加密算法 DES 加密数据，用数字签名认证发送端对数据进行完整性检测。同样，建立安全关联的过程也是协商安全参数和密钥分配协议的过程，双方最后确定的安全参数如下：

- 安全协议　ESP。
- 加密算法　AES。
- 认证算法　HMAC-MD5-96。
- SPI　12345678H。
- 主密钥 $MK=YR_{21}^{XR_{11}} \bmod q=YR_{11}^{XR_{21}} \bmod q$。

SPI 由单向安全关联的接收端分配，如图 6.17 建立的路由器 R_1 至路由器 R_2 的安全关联，由路由器 R_2 分配 SPI。

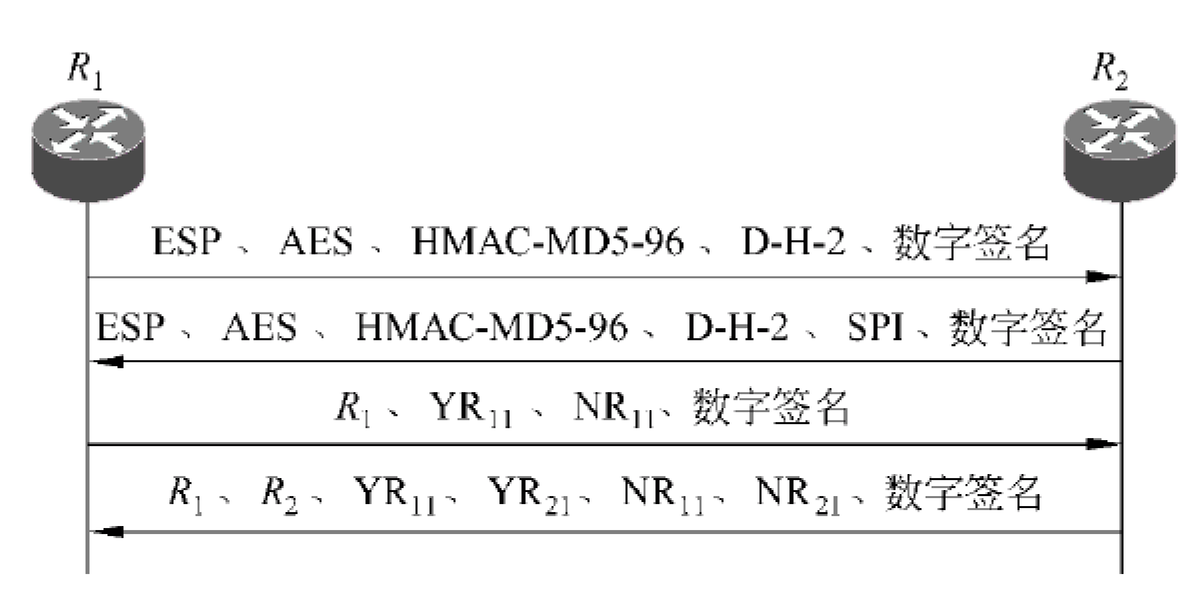


图 6.17　建立安全关联的过程

2. 安全传输数据

安全关联的发送端（这里为路由器 R_1）通过分组过滤器来绑定安全关联，接收端通过目的地址、SPI 和安全协议绑定安全关联。

当路由器 R_1 通过端口 1 接收到源 IP 地址=193.1.1.1、目的 IP 地址=193.1.2.5 的 IP 分组，用目的 IP 地址 193.1.2.5 检索路由表，确定通往下一跳的路径为隧道，该 IP 分组被封装成隧道格式。在路由器端口 2 用隧道格式的多个字段值匹配分组过滤器，确定隧道格式符合过滤规则：源 IP 地址=200.1.1.1/32 • AND • 目的 IP 地址=200.1.2.1/32，用表 6.4 所示的和该过滤规则绑定的安全关联进行图 6.18 所示的 ESP 隧道模式封装处理过程。将内层 IP 分组封装成 ESP 报文，整个内层 IP 分组作为 ESP 报文的净荷字段。对 ESP 报文的净荷字段和尾部进行加密运算，并对密文和 ESP 首部进行 HMAC-MD5-96 运算，生成 96 位的消息认证码。最后对 ESP 报文加上外层 IP 首部，将其封装为 ESP 隧道模式，通过路由器端口 2 发送出去。

表 6.4 路由器 R_1 安全关联绑定关系

源 IP 地址＝200.1.1.1/32 • AND • 目的 IP 地址＝200.1.2.1/32					
SPI	安全协议	加密算法	认证算法	加密密钥	认证密钥
12345678H	ESP	AES	HMAC-MD5-96	K_1	K_2

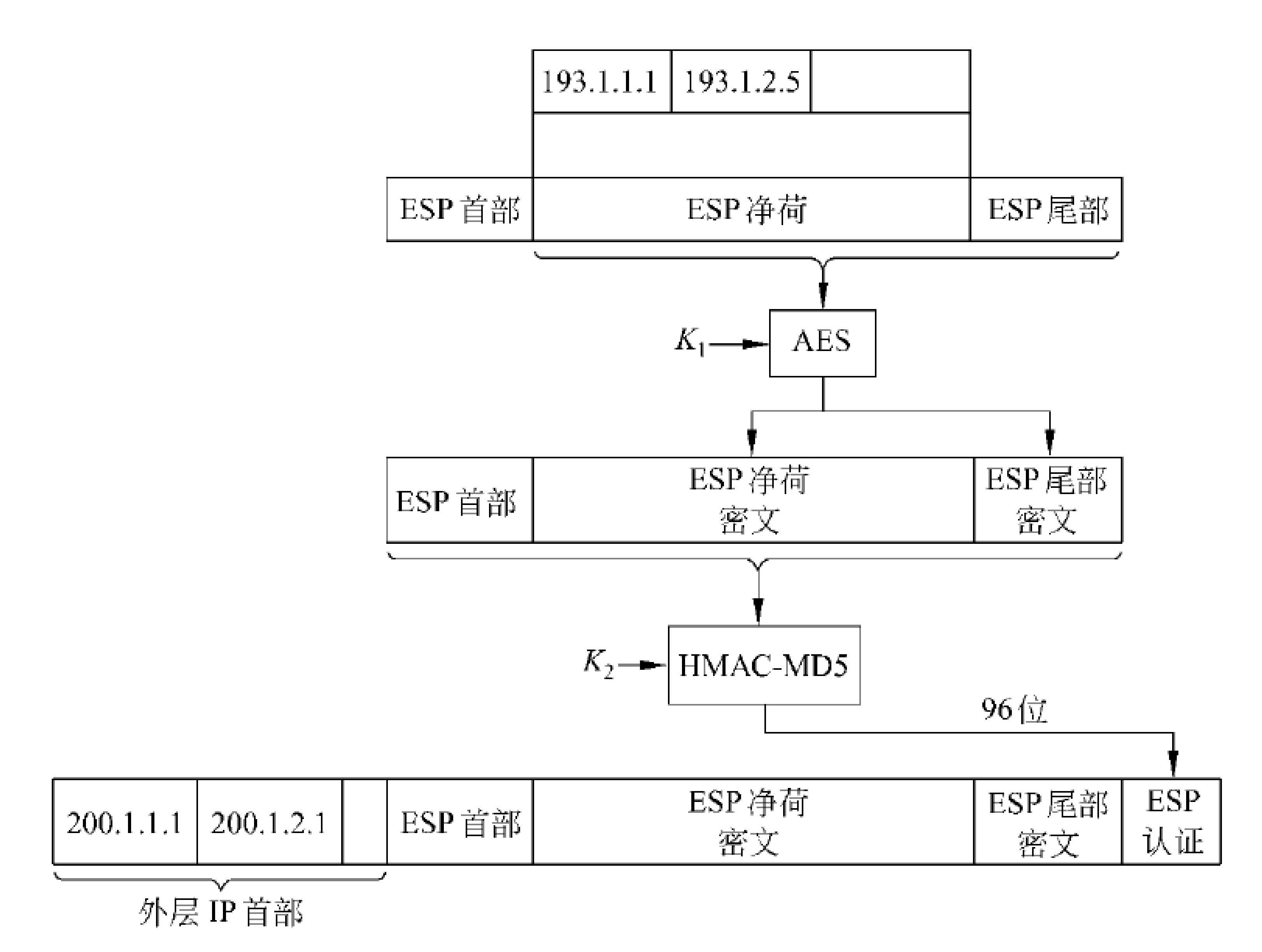


图 6.18 ESP 隧道模式封装、处理过程

当路由器 R_2 通过端口 2 接收到隧道模式的 ESP 报文，首先用目的 IP 地址(200.1.2.1)、协议类型字段指定的安全协议(ESP)和 ESP 首部中的 SPI(12345678H)去匹配安全关联，找到表 6.5 所示的安全关联，然后进行和图 6.18 所示的相反的处理过程：剥离外层 IP 首部，用认证密钥 K_2 对包括 ESP 首部和密文的 ESP 报文进行 HMAC-MD5 运算，取高 96 位和 ESP 认证字段进行比较，如果相等，表明 ESP 报文传输过程中未被篡改，否则，作相应的出错处理。用密钥 K_2 和 AES 解密过程对密文解密，获取内层 IP 分组，用该 IP 分组的目的地址检索路由表，找到对应路由项，将该 IP 分组封装成 MAC 帧后，从路由器端口 1 转发出去。

表 6.5 路由器 R_2 安全关联绑定关系

目的 IP 地址＝200.1.2.1/32 • AND • SPI＝12345678H • AND • 安全协议＝ESP					
SPI	安全协议	加密算法	认证算法	加密密钥	认证密钥
12345678H	ESP	AES	HMAC-MD5-96	K_1	K_2

6.3　虚拟接入网络

6.3.1　网络结构

虚拟接入网络结构如图 6.19 所示，企业内部网络采用本地 IP 地址 193.1.2.0/24，和 Internet 相连的路由器端口分配全球 IP 地址 100.1.2.1，企业内部网络连接 Internet 的路由器相当于内部网络的网络接入服务器，承担对远程接入用户进行身份认证、内部网络本地 IP 地址分配等功能。当远程接入用户需要接入企业内部网络时，建立远程接入用户和企业内部网络路由器之间的点对点链路，并基于点对点链路和 PPP 完成对远程接入用户的身份认证、内部网络本地 IP 地址分配等过程。远程接入用户通过拨号接入方式接入内部网络，但远程接入用户并不直接建立和内部网络中网络接入服务器之间的点对点语音信道，而是建立和本地 ISP 接入服务器之间的语音信道，再由本地 ISP 接入服务器建立和内部网络中网络接入服务器之间的基于 IP 网络的第 2 层隧道，本地 ISP 接入服务器负责将与远程接入用户之间的点对点语音信道和与内部网络中的网络接入服务器之间的基于 IP 网络的第 2 层隧道交接在一起，构成用于在远程接入用户和内部网络中的网络接入服务器之间交换 PPP 帧的点对点链路。

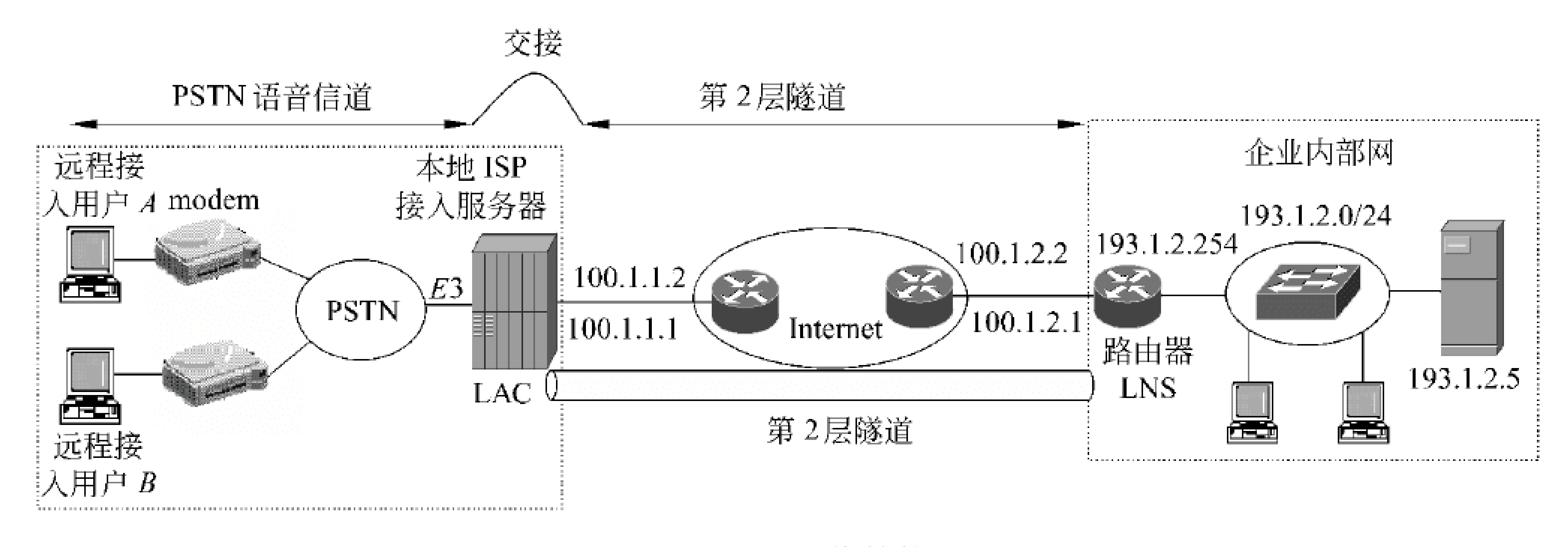


图 6.19　网络结构

6.3.2　第 2 层隧道和第 2 层隧道协议

第 2 层隧道用于传输链路层帧，其功能等同于物理层链路，因此，也把第 2 层隧道称作虚拟线路。第 2 层隧道协议（Layer Two Tunneling Protocol，L2TP）是一种动态建立基于 IP 网络的第 2 层隧道或虚拟线路的信令协议，目前常见的是第 3 版第 2 层隧道协议，简写为 L2TPv3。图 6.19 所示的网络结构中，由 L2TPv3 动态建立基于 IP 网络的、等同于点对点语音信道的 L2TP 接入集中器（L2TP Access Concentrator，LAC）和 L2TP 网络服务器（L2TP Network Server，LNS）之间的第 2 层隧道，由于本地 ISP 接入服务器允许多个想要接入内部网络的远程用户与其同时建立语音信道，因此，被称为 L2TP 接入集中器（LAC），而内部网络连接 Internet 的路由器对远程接入用户而言就是接入服务器，因此，被称为 L2TP 网络服务器（LNS）。在由点对点语音信道和第 2 层隧道交接后组成的

远程接入用户和 LNS 之间的虚拟线路基础上，通过建立远程接入用户和 LNS 之间的 PPP 链路，由 LNS 基于 PPP 完成对远程接入用户的身份认证和内部网络本地 IP 地址分配，实现远程接入用户接入企业内部网络的过程。

1. 第 2 层隧道报文格式

通过点对点语音信道传输的 PPP 帧的格式如图 6.20 所示，由于 PPP 帧在点对点链路上传输，因此，不需要链路层地址信息，地址字段值固定为 FF，当 PPP 作为面向字符的链路层协议时，由物理层实现字符同步，由链路层实现帧定界。

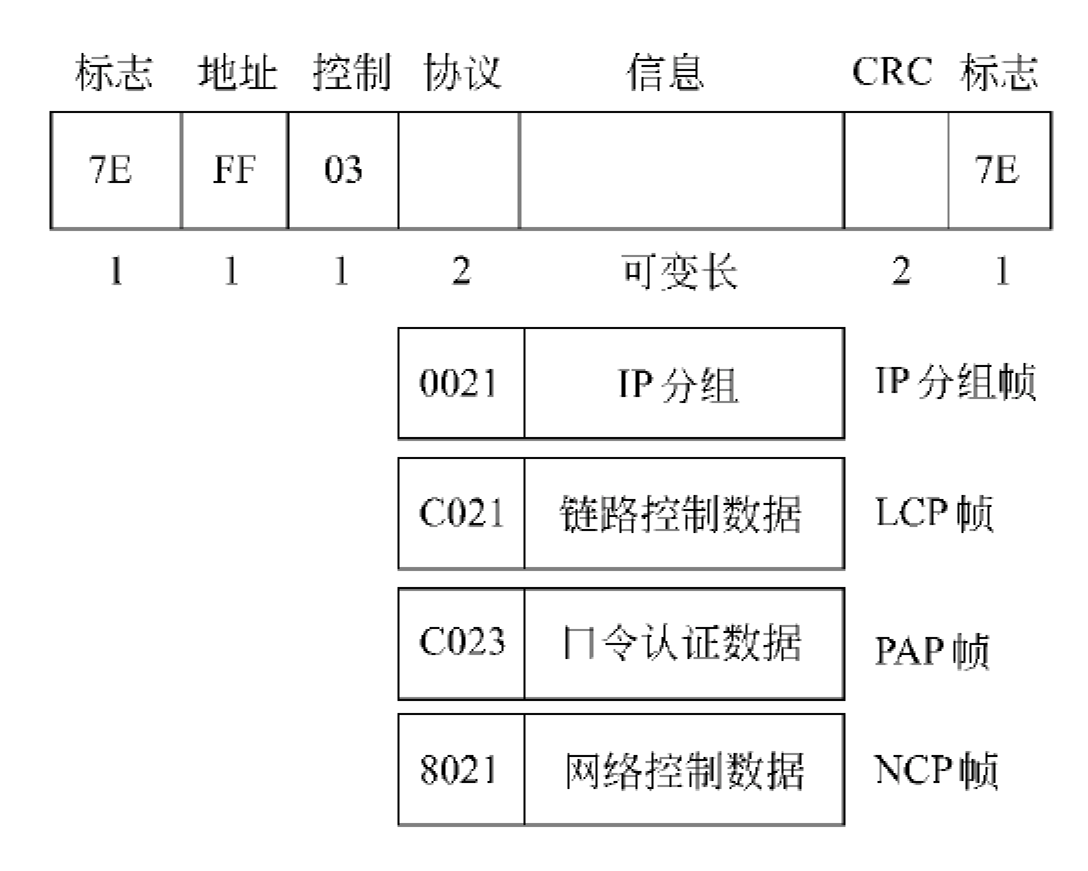


图 6.20 PPP 帧结构

当通过基于 IP 网络的第 2 层隧道传输 PPP 帧时，需要将 PPP 帧封装为图 6.21 所示的第 2 层隧道格式。第 2 层隧道格式直接作为以第 2 层隧道两端 IP 地址为源和目的 IP 地址的 IP 分组的净荷的封装形式称为第 2 层隧道报文。

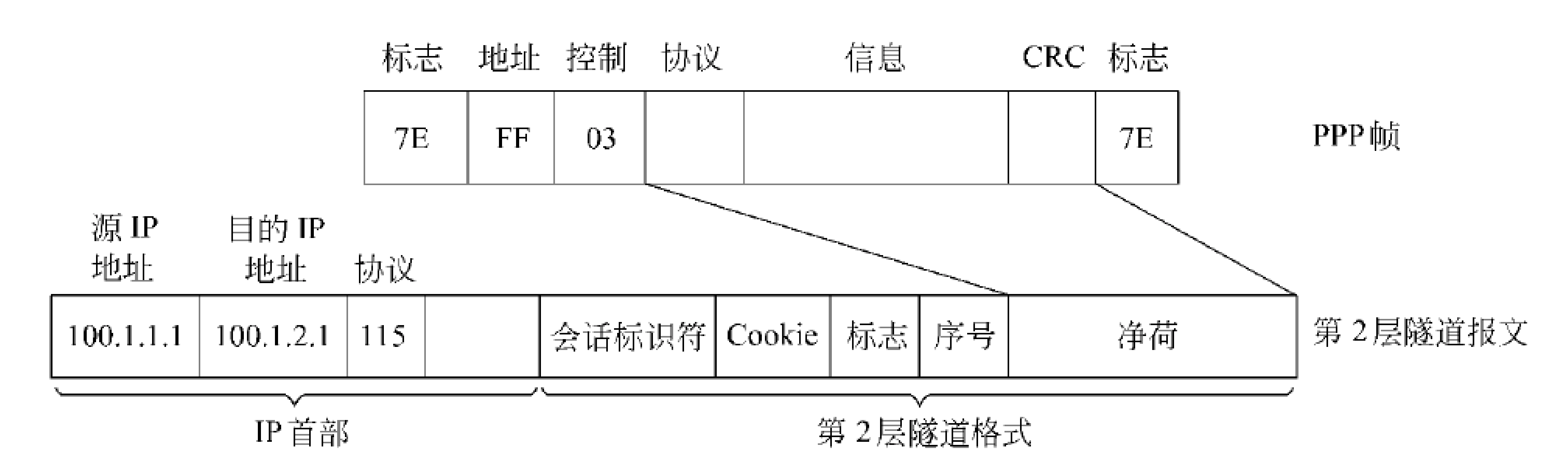


图 6.21 PPP 帧封装成第 2 层隧道报文的过程

第 2 层隧道格式中各个字段的含义如下。

- 会话标识符：32 位，唯一标识第 2 层隧道，其功能等同于标识语音信道的时隙号。由于会话标识符具有本地意义，第 2 层隧道格式中的会话标识符用于接收端确定传输数据的虚拟线路。
- Cookie：32 位或 64 位，它是会话标识符的补充，也用于标识传输数据的第 2 层隧道，Cookie 有着比会话标识符更强的随机性，因此，除非攻击者能够截获经过第 2 层隧道传输的数据，否则，很难伪造用于在特定第 2 层隧道中传输的第 2 层隧道

报文。Cookie 同样具有本地意义，第 2 层隧道格式中的 Cookie 用于接收端确定传输数据的虚拟线路。

- 标志：8 位，目前只定义 1 位标志位 S，当该位标志位置 1 时，表明第 2 层隧道格式包含序号字段。
- 序号：24 位，发送端为每一条第 2 层隧道设置序号计数器，建立第 2 层隧道时，序号计数器为 0，发送端发送数据时，将序号计数器值作为第 2 层隧道格式的序号字段值，每发送一帧数据，序号计数器增 1，因此，经过同一第 2 层隧道传输的数据，序号是递增的。设置序号的目的是保证经过第 2 层隧道传输的数据按序、没有重复地到达接收端。由于第 2 层隧道仿真点对点链路，而基于点对点链路的链路层协议有着按序、不重复接收相同链路层帧的特性，但基于 IP 网络的第 2 层隧道通过 IP 网络传输封装成 IP 分组的第 2 层隧道报文时，无法确保经过 IP 网络传输的第 2 层隧道报文按序、不重复地到达接收端，因此，接收端需要设置一个期待接收序号计数器，当正确接收到某个第 2 层隧道报文时，将该第 2 层隧道报文携带的序号值增 1 后作为期待接收序号计数器值，接收到的第 2 层隧道报文当且仅当携带的序号值大于等于期待接收序号计数器值时，接收端才继续予以处理；否则，接收端将丢弃该第 2 层隧道报文。

2. 建立第 2 层隧道过程

虽然第 2 层隧道的功能等同于点对点链路，但由于第 2 层隧道是基于 IP 网络的，由 IP 网络保证第 2 层隧道两端之间的 IP 分组传输路径，因此，建立第 2 层隧道的过程和建立语音信道这样点对点物理链路的过程不同，它不存在建立实际的第 2 层隧道两端之间物理传输路径的过程，而只是一个协商第 2 层隧道的类型、在第 2 层隧道两端分配会话标识符、Cookie 的过程。

由于建立第 2 层隧道所需要的控制消息封装成 IP 分组后，经过 IP 网络进行传输，而 IP 网络本身只能提供尽力而为服务，因此，无法保证控制消息在第 2 层隧道两端正确传输。TCP 提供了在 IP 网络上可靠传输的机制，因此，L2TPv3 在经过 IP 网络传输控制消息的过程中借鉴了 TCP 确认应答和重传机制，这样，建立第 2 层隧道过程分为两个阶段，第一个阶段是建立控制连接，第 2 个阶段是通过控制连接实现用于建立第 2 层隧道的控制消息的可靠传输，并因此完成第 2 层隧道的建立过程。多个第 2 层隧道建立过程，只需一个控制连接建立过程，多个第 2 层隧道建立过程中涉及的控制消息通过同一个控制连接实现可靠传输，因此，控制连接建立过程有点类似于 TCP 连接建立过程，但在控制连接建立过程中可以实现控制连接两端的相互认证和其他参数的协商过程，这是 TCP 连接所无法实现的。

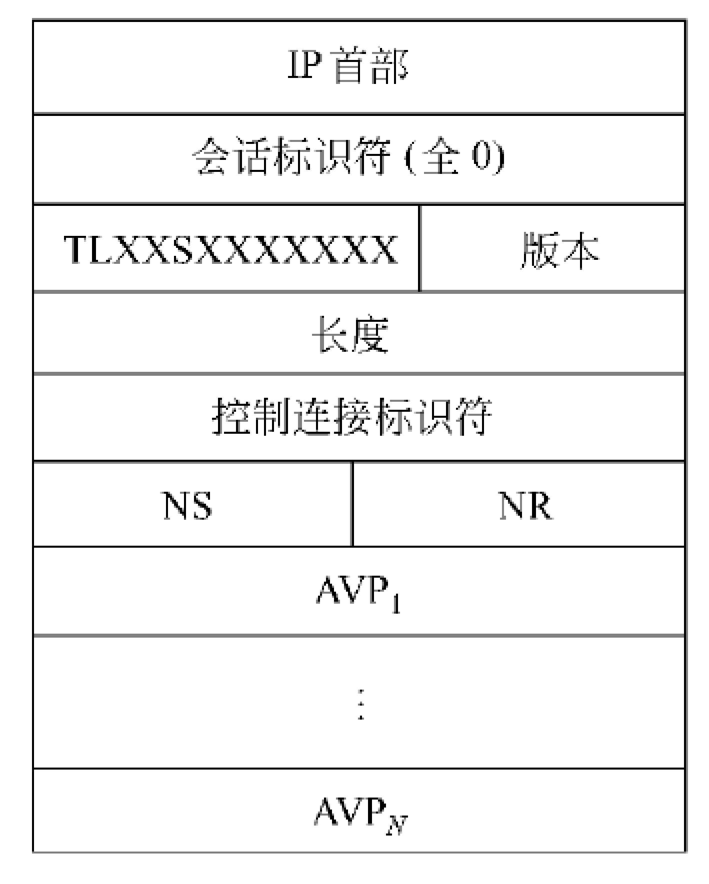


图 6.22　L2TPv3 控制消息格式

图 6.22 是封装成 IP 分组的 L2TPv3 控制消息格式，全 0 的会话标识符表明是控制消息，而不是一般链路层帧，因此，图 6.21 中的会话标识符不允许全 0，表

明不能用全 0 标识一个实际的虚拟线路(第 2 层隧道)。*T*、*L* 和 *S* 标志位必须置 1,*T* 标志位置 1 表明是控制消息,*L* 标志位置 1 表明长度字段有效,*S* 标志位置 1 表明发送和接收序号字段(NS 和 NR)有效。版本字段给出 L2TP 的版本号,这里是 3,表明是 L2TPv3。长度字段给出从 *T* 标志位起到控制消息结束所包含的字节数。控制连接标识符用于接收端确定传输控制消息的控制连接,它具有本地意义。序号(NS)和接收序号(NR)的含义和 TCP 首部中序号和确认序号相同,用于确认应答和重传机制。属性值对(Attribute Value Pair,AVP)用于传输建立控制连接或第 2 层隧道所需要的参数。

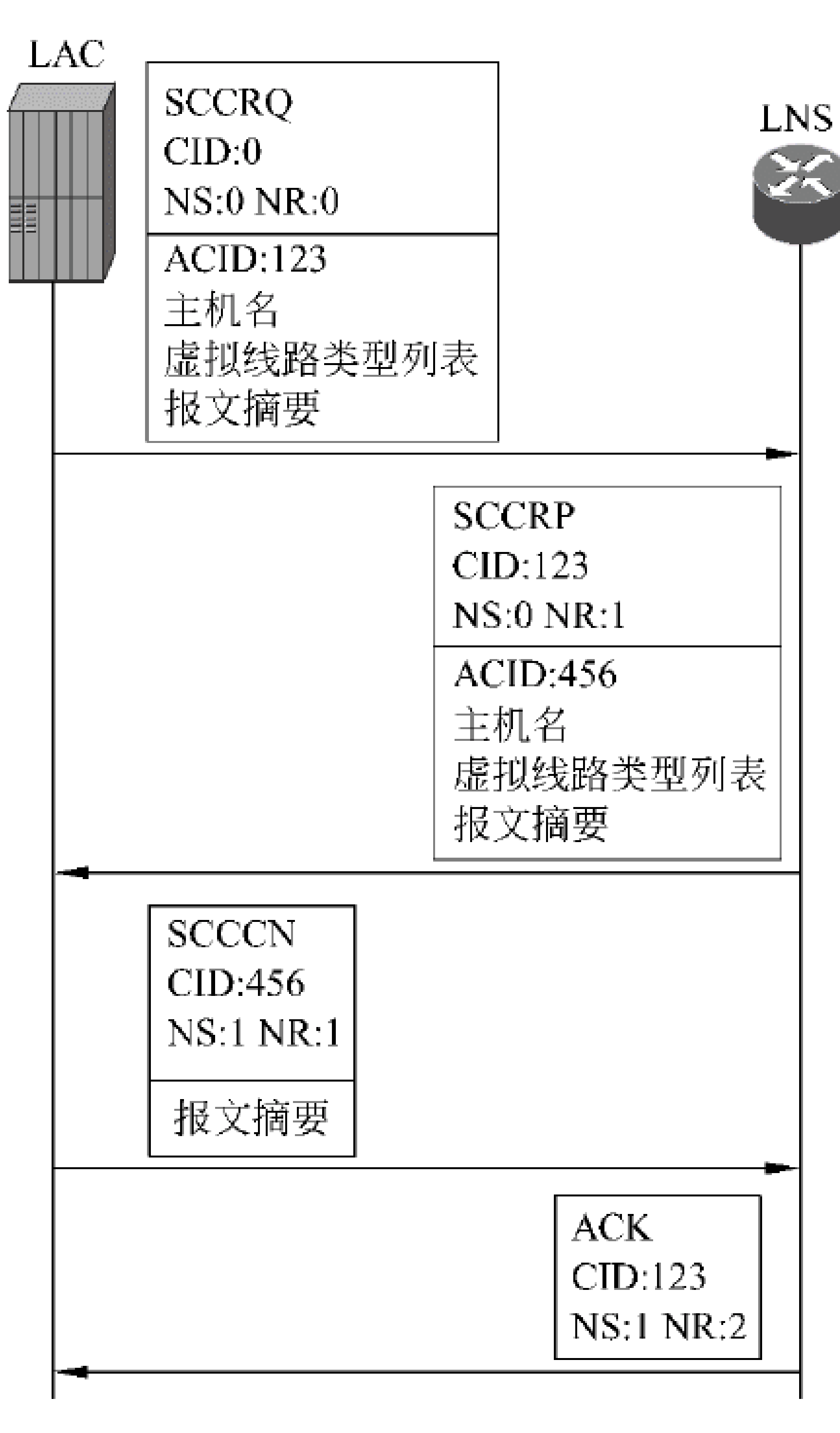


图 6.23 控制连接建立过程

1) 控制连接建立过程

控制连接建立过程如图 6.23 所示。通过发送启动控制连接请求(Start Control Connection Request,SCCRQ)消息开始控制连接建立过程,由于控制连接尚未建立,因此,该消息的控制连接标识符(CID)为 0,发送和接收序号(NS 和 NR)的初值为 0。发送 SCCRQ 消息的 LAC 必须为该控制连接分配本地控制连接标识符(ACID=123),本地控制连接标识符通过 AVP 给出,它是 LAC 唯一标识该控制连接的标识符,以后,通过该控制连接发送给 LAC 的控制消息必须以该本地控制连接标识符为控制连接标识符。因此,当 LNS 同意建立控制连接,向 LAC 发送启动控制连接响应(Start Control Connection Reply,SCCRP)消息时,其中的控制连接标识符必须是 LAC 分配的本地控制连接标识符 123。LNS 同样需要在 SCCRP 中分配本地连接标识符(ACID=456),在 LNS 分配本地连接标识符后,LAC 所有发送给 LNS 的控制消息都以该本地连接标识符为控制连接标识符。LAC 在接收到表明 LNS 同意建立控制连接的 SCCRQ 后,通过向 LNS 发送启动控制连接建立(Start Control Connection Connected,SCCCN)消息完成控制连接建立过程,LAC 和 LNS 对接收到的任何控制消息必须回送确认应答,和 TCP 一样,确认应答可以捎带在发送给对方的控制消息中,如 SCCRP 和 SCCCN 消息,也可发送专门的确认应答消息,如最后的 ACK 消息。

建立控制连接过程除了双方协商产生控制连接标识符外,还需协商产生双方共同支持的虚拟线路类型,虚拟线路类型是指虚拟线路支持的链路层帧格式,如 PPP 帧和 MAC 帧,因此,也有了对应的点对点虚拟线路和以太网虚拟线路。LAC 必须在 SCCRQ 中的虚拟线路类型列表中列出它所支持的所有虚拟线路类型,如果 LNS 支持的虚拟线路类型和 LAC 在 SCCRQ 中的虚拟线路类型列表中列出的虚拟线路类型存在交集,就将交集作为 LNS 发送给 LAC 的 SCCRP 中的虚拟线路类型列表,否则,控制连接建立失败。

建立控制连接过程需要完成的另一个功能是双方身份认证，LAC发送给LNS的SCCRQ中携带标识LAC的主机名和报文摘要，报文摘要＝HAMC-MD5或HMAC-SHA-1(控制消息)，计算基于密钥的报文摘要所需要的共享密钥通过配置给出。为了防止攻击者伪造控制消息的报文摘要，LAC发送SCCRQ时还需携带随机数SN，SN也通过AVP给出。LNS发送给LAC的SCCRP和LAC发送给LNS的SCCCN中的报文摘要＝HMAC-MD5或HMAC-SHA-1(SN‖RN‖控制消息)，其中SN是LAC产生的随机数，RN是LNS产生的随机数，这样，保证攻击者难以伪造报文摘要。LAC和LNS接收到对方发送的控制消息后，都重新计算报文摘要，并将计算结果和控制消息携带的报文摘要比较，如果相等，表明发送端身份合法且控制消息传输过程中未被篡改。由于虚拟线路是基于IP网络，而IPSec协议能够对通过IP网络传输的IP分组提供更高的安全性，因此，在由IPSec保障虚拟线路的安全性的情况下，L2TPv3的认证和数据完整性检测功能可以去掉。

2) 第2层隧道建立过程

建立第2层隧道的过程就是双方协调产生会话标识符和确定第2层隧道的虚拟线路类型的过程，如图6.24所示，由LAC发送入呼叫请求(Incoming Call Request，ICRQ)消息开始第2层隧道的建立过程，ICRQ中通过AVP给出LAC分配的本地会话标识符(ALSID＝678)和指定的虚拟线路类型：PPP虚拟线路。表示以后所有通过虚拟线路发送给LAC的数据均需先封装成PPP帧格式，然后再将PPP帧封装成图6.21所示的第2层隧道格式，其中会话标识符必须为LAC分配的本地会话标识符678。为了更好地防止中继攻击，可以用会话标识符和Cookie一起唯一标识某个会话，这种情况下，LAC不但需要分配本地会话标识符，还需分配本地Cookie，但Cookie不是必需的，因此，图6.24中没有列出。LNS接收到LAC发送的ICRQ，如果支持ICRQ中列出的虚拟线路类型且同意建立虚拟线路，向LAC发送入呼叫响应(Incoming Call Reply，ICRP)消息，ICRP中同样通过AVP给出LNS分配的本地会话标识符(ALSID＝789)和虚拟线路类型(PPP虚拟线路)，表示以后所有通过虚拟线路发送给LNS的数据均需先封装成PPP帧格式，然后再将PPP帧封装成图6.21所示的第2层隧道格式，其中会话标识符必须为LNS分配的本地会话标识符789。ICRP中用远端会话标识符(ARSID＝678)给出LAC分配的本地会话标识符，以此验证LNS是否正确接收了LAC发送的ICRQ。LAC接收到LNS发送的ICRP，如果ICRP中的远

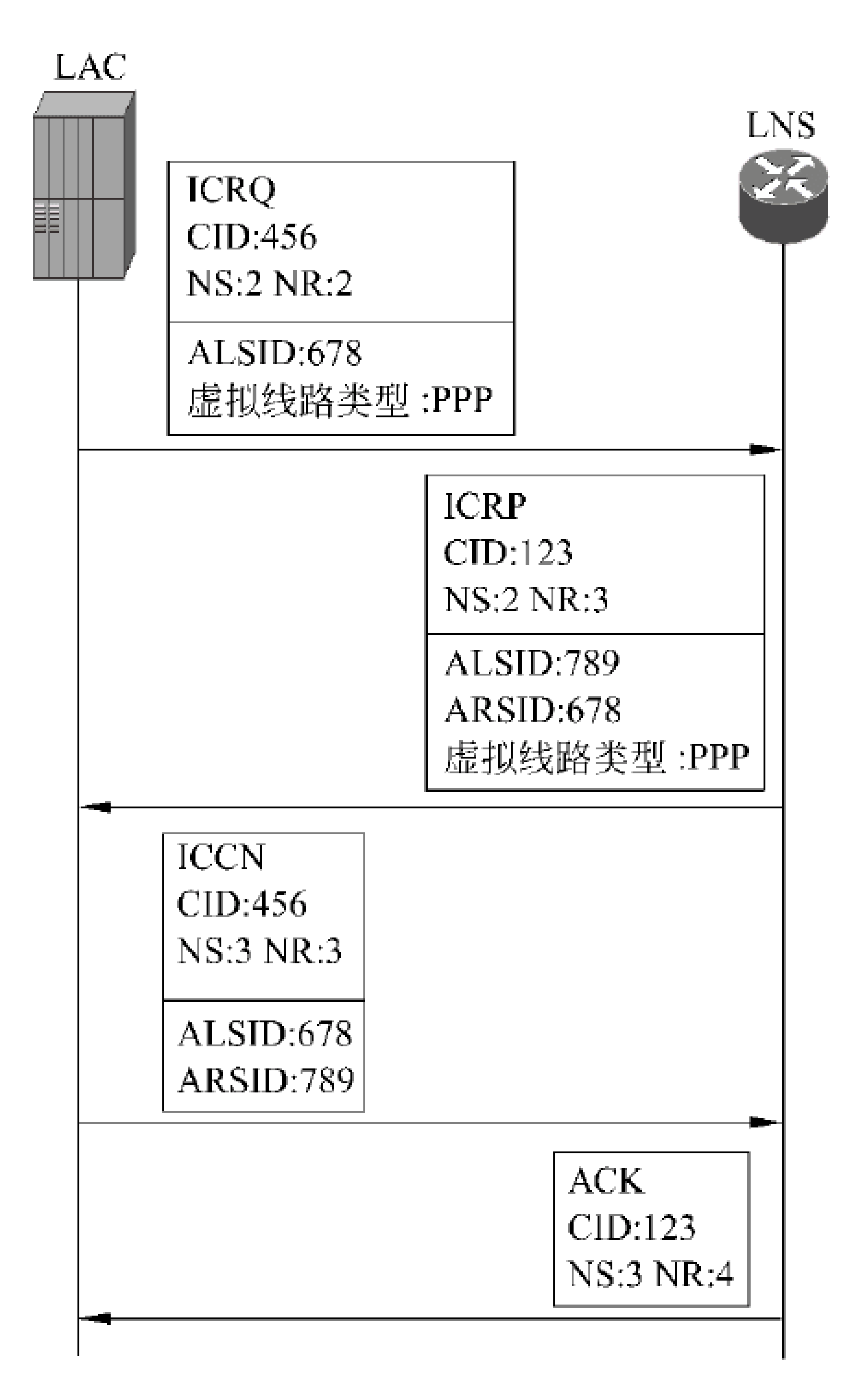


图6.24　第2层隧道建立过程

端会话标识符和虚拟线路类型与本地分配的会话标识符和本地指定的虚拟线路类型相同,通过发送入呼叫建立(Incoming Call Connected,ICCN)消息表示第 2 层隧道成功建立,为了让 LNS 验证 LAC 是否正确接收到 LNS 发送的 ICRP,ICCN 中分别通过本地和远端会话标识符给出 LAC 分配的本地会话标识符和 LNS 分配的本地会话标识符。和控制连接建立过程一样,由于没有控制消息可以捎带 LNS 对 ICCN 的确认应答,用专门的 ACK 作为 ICCN 的确认应答。

6.3.3 远程接入用户接入内部网络过程

远程接入用户接入内部网络过程如图 6.25 所示,它由建立远程接入用户和 LAC 之间的语音信道、建立远程接入用户和 LAC 之间的 PPP 链路、建立 LAC 和 LNS 之间的第 2 层隧道、建立远程接入用户和 LNS 之间的 PPP 链路、LNS 为远程接入用户分配内部网络本地 IP 地址等步骤组成。

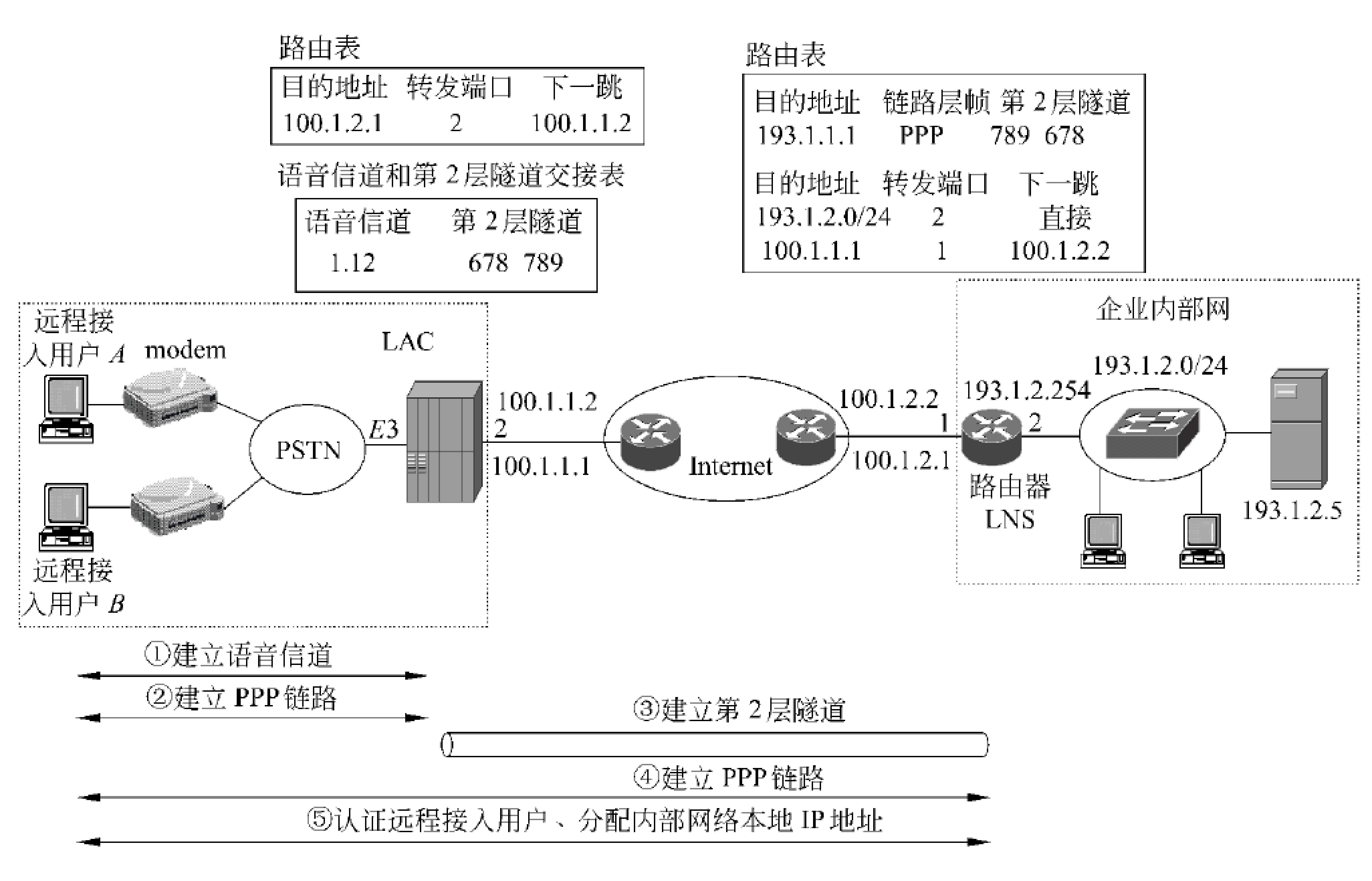


图 6.25 远程接入用户接入内部网络过程

1. 建立远程接入用户和 LAC 之间的语音信道

远程接入用户通过呼叫连接建立过程建立远程接入用户和 LAC 之间的语音信道,LAC 连接 PSTN 的 $E3$ 链路中必须为该语音信道分配一个时隙,这里假定为 1.12,LAC 可以用时隙 1.12 唯一标识远程接入用户和 LAC 之间的语音信道,而该语音信道就是在远程接入用户和 LAC 之间传输 PPP 帧的点对点物理链路。

2. 建立远程接入用户和 LAC 之间的 PPP 链路

通过远程接入用户和 LAC 之间建立的语音信道,远程接入用户和 LAC 之间通过交换 PPP LCP 帧完成 PPP 链路建立过程,通过建立 PPP 链路过程,远程接入用户和 LAC

完成参数协商，并由 LAC 指定认证协议，远程接入用户根据 LAC 指定的认证协议向 LAC 传输认证信息，由 LAC 完成对远程接入用户的身份认证，并确定远程接入用户的网络接入服务器为 LNS。

3. 建立 LAC 和 LNS 之间的第 2 层隧道

LAC 一旦确定本次接入的网络服务器为 LNS，开始 LAC 和 LNS 之间的第 2 层隧道的建立过程，如果已经存在 LAC 和 LNS 之间的控制连接，直接开始图 6.24 所示的第 2 层隧道建立过程；否则，先通过图 6.23 所示的过程建立 LAC 和 LNS 之间的控制连接。在成功建立 LAC 和 LNS 之间的第 2 层隧道后，LAC 将标识连接远程接入用户的语音信道的时隙号 1.12 和标识 LAC 和 LNS 之间第 2 层隧道的本地和远端会话标识符绑定在一起，作为 LAC 交接表中一项。此时，远程接入用户和 LNS 之间的虚拟点对点链路成功建立，它由远程接入用户和 LAC 之间的语音信道与 LAC 和 LNS 之间的第 2 层隧道组成。

4. 建立远程接入用户和 LNS 之间的 PPP 链路

一旦成功建立远程接入用户和 LNS 之间的虚拟点对点链路，就可通过在远程接入用户和 LNS 之间交换 PPP LCP 帧建立 PPP 链路，指定认证协议，远程接入用户根据指定的认证协议向 LNS 传输认证信息，由 LNS 完成对远程接入用户的身份认证。值得指出的是：远程接入用户发送给 LNS 的 PPP LCP 帧在 LAC 封装成图 6.21 所示的第 2 层隧道报文后，才能通过基于 IP 网络的第 2 层隧道传输给 LNS，反之，LNS 发送给远程接入用户的 PPP LCP 帧封装成图 6.21 所示的第 2 层隧道报文后，才能通过基于 IP 网络的第 2 层隧道传输给 LAC，LAC 从第 2 层隧道报文中分离出 PPP LCP 帧，通过和远程接入用户之间的语音信道将 PPP LCP 帧发送给远程接入用户。

5. 分配内部网络的本地 IP 地址

在成功建立远程接入用户和 LNS 之间的 PPP 链路，并由 LNS 完成对远程接入用户的身份认证后，LNS 和远程接入用户之间通过交换 PPP IPCP 帧完成对远程接入用户的 IP 地址分配，LNS 从本地 IP 地址池中选择一个 IP 地址(这里为 193.1.1.1)分配给远程接入用户，并将分配给远程接入用户的 IP 地址与 LNS 和远程接入用户之间的虚拟点对点链路绑定在一起，作为路由表中一项，LNS 通过第 2 层隧道的本地和远程会话标识符唯一标识 LNS 和远程接入用户之间的虚拟点对点链路。

6.3.4 数据传输过程

当远程接入用户访问内部网络中的服务器时，远程接入用户构建以 193.1.1.1 为源 IP 地址，193.1.2.5 为目的 IP 地址的 IP 分组，再将 IP 分组封装成 PPP IP 帧，通过远程接入用户和 LAC 之间的语音信道将 PPP 帧传输给 LAC，对于远程接入用户至内部网络服务器的内部网络传输路径而言，LAC 相当于物理层中继设备，它从通过时隙 1.12 接收到的字节流中分离出 PPP IP 帧，重新封装成等同于物理层链路的第 2 层隧道所要求的格式，因此，PPP IP 帧经过内部网络传输路径的传输过程中，LAC 只是完成了两种不同的物理层传输格式的转换。但第 2 层隧道是基于 IP 网络的虚拟线路，因此，并不能直接通过虚拟线路传输构成 PPP IP 帧的字节流，而是必须把 PPP IP 帧封装成图 6.26 所示的第

2 层隧道报文，其中，会话标识符为 LNS 的本地会话标识符 789。当 LAC 将以全球 IP 地址 100.1.1.1 为源 IP 地址、100.1.2.1 为目的 IP 地址的第 2 层隧道报文传输给 Internet 时，它是 Internet 的边缘路由器，用目的 IP 地址 100.1.2.1 检索路由表，找到 Internet 中的下一跳路由器，把第 2 层隧道报文传输给下一跳路由器。第 2 层隧道报文经过 Internet 的逐跳转发，到达 LNS，LNS 首先从第 2 层隧道报文中分离出 PPP IP 帧，再从 PPP IP 帧中分离出 IP 分组，用 IP 分组的目的 IP 地址 193.1.2.5 检索路由表，获知目的终端位于和其直接相连的以太网中，将 IP 分组封装成 MAC 帧后，通过以太网传输给服务器，完成远程接入用户至内部网络服务器的 IP 分组传输过程。IP 分组传输过程中各个中继设备的协议转换过程如图 6.27 所示。

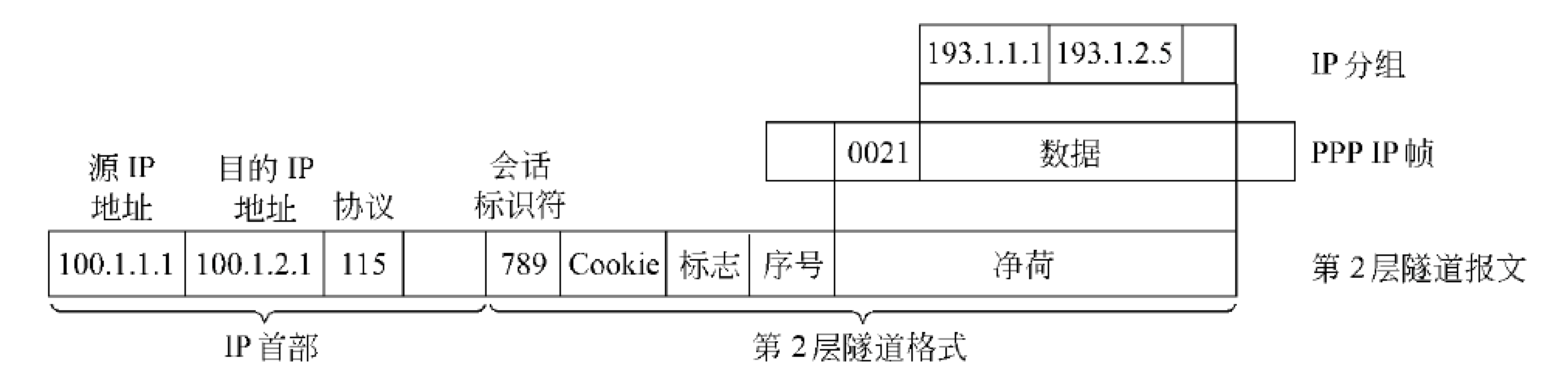


图 6.26 IP 分组封装成第 2 层隧道报文过程

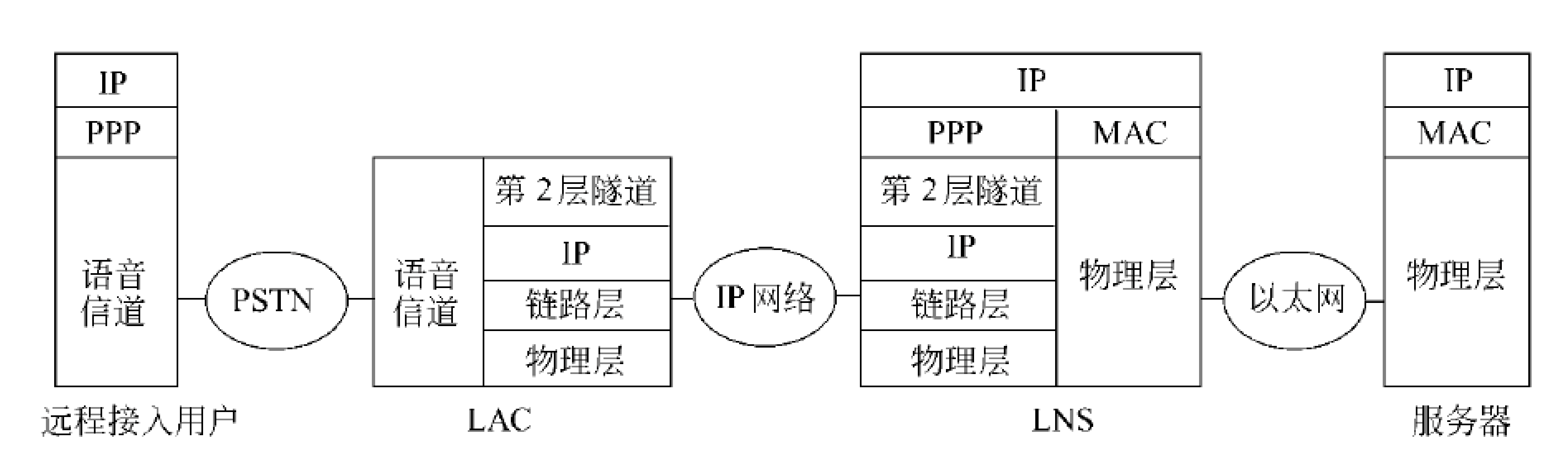


图 6.27 协议转换过程

当内部网络服务器传输数据给远程接入用户时，构建以 193.1.2.5 为源 IP 地址，193.1.1.1 为目的 IP 地址的 IP 分组，再将 IP 分组封装成 MAC 帧，通过以太网传输给默认网关 LNS，LNS 从 MAC 帧中分离出 IP 分组，用 IP 分组的目的 IP 地址 193.1.1.1 检索路由表，找到图 6.25 所示的路由项，获知连接远程接入用户的链路是第 2 层隧道，将 IP 分组封装成 PPP IP 帧，再将 PPP IP 帧封装层第 2 层隧道报文，当然，第 2 层隧道报文中的源 IP 地址为 LNS 连接 Internet 的端口的全球 IP 地址 100.1.2.1，目的 IP 地址为 LAC 连接 Internet 的端口的全球 IP 地址 100.1.1.1，会话标识符为 LAC 本地会话标识符 678。第 2 层隧道报文经过 Internet 到达 LAC，LAC 作为物理层中继设备，需要完成传输 PPP IP 帧的物理层格式转换，因此，从第 2 层隧道报文中分离出 PPP IP 帧，加上 PPP IP 帧的首部和尾部信息，将构成 PPP IP 帧的字节流通过时隙号为 1.12 的语音信道发送出去。远程接入用户通过语音信道接收到 PPP IP 帧，从中分离出 IP 分组，完成内部网络服务器至远程接入用户的 IP 分组传输过程。IP 分组传输过程中各个中继设备的协

议转换过程如图 6.27 所示。

6.3.5　安全机制

如果经过 IP 网络传输时采用 IPSec 安全机制，首先必须在 LAC 和 LNS 之间建立安全关联，由于安全关联是单向的，因此，如果要实现 LAC 和 LNS 之间双向安全传输，必须建立双向安全关联，表 6.6 和表 6.7 所示的是和 LAC 至 LNS 安全关联相关的安全参数。建立安全关联的过程和 6.2.3 节讨论的过程相同，这里不再赘述。

表 6.6　LAC 安全关联绑定关系

源 IP 地址＝100.1.1.1/32 • AND • 目的 IP 地址＝100.1.2.1/32					
SPI	安全协议	加密算法	认证算法	加密密钥	认证密钥
12345678H	ESP	AES	HMAC-MD5-96	K_1	K_2

表 6.7　LNS 安全关联绑定关系

目的 IP 地址＝100.1.2.1/32 • AND • SPI＝12345678H • AND • 安全协议＝ESP					
SPI	安全协议	加密算法	认证算法	加密密钥	认证密钥
12345678H	ESP	AES	HMAC-MD5-96	K_1	K_2

第 2 层隧道安全机制采用 ESP 运输模式，LAC 根据表 6.6 所示的安全参数加密第 2 层隧道报文的过程如图 6.28 所示。IP 首部中的协议字段值改为 50，表明 IP 分组净荷是 ESP 报文，ESP 首部中的下一个首部字段值为 17，表明 ESP 报文净荷是 UDP 报文，UDP 报文的目的端口号为 1701，表明 UDP 报文净荷是第 2 层隧道格式。当 PPP IP 帧封装成第 2 层隧道格式时，可以将第 2 层隧道格式直接作为 IP 分组净荷，如图 6.26 所示，也可以先将第 2 层隧道格式作为 UDP 报文净荷，用目的端口号 1701 表明 UDP 净荷是第 2 层隧道格式。当使用 ESP 运输模式时，ESP 报文净荷通常是运输层报文，因此，需将第 2 层隧道格式先封装成 UDP 报文。

6.3.6　虚拟接入网络——自愿隧道

1. 远程接入用户接入内部网络过程

前面讨论的虚拟接入网络由 LAC 启动第 2 层隧道建立过程，激发 LAC 启动第 2 层隧道建立过程的事件是远程接入用户的入呼叫过程，LAC 一旦检测到远程接入用户的入呼叫信令，建立和远程接入用户之间的语音信道，完成对远程接入用户的身份认证，自动启动和 LNS 之间的第 2 层隧道的建立过程，由于这种接入方式由 LAC 自动启动和 LNS 之间的第 2 层隧道的建立过程，被称为是强制隧道方式，在强制隧道方式，LAC 和 LNS 之间的第 2 层隧道对远程接入用户是透明的。实际应用中，希望接入企业内部网络的用户可能通过多种方式接入 Internet，如以太网、ADSL 等，这些接入方式需要直接在远程接入用户和 LNS 之间建立第 2 层隧道，并以第 2 层隧道为点对点链路，通过 PPP 完成

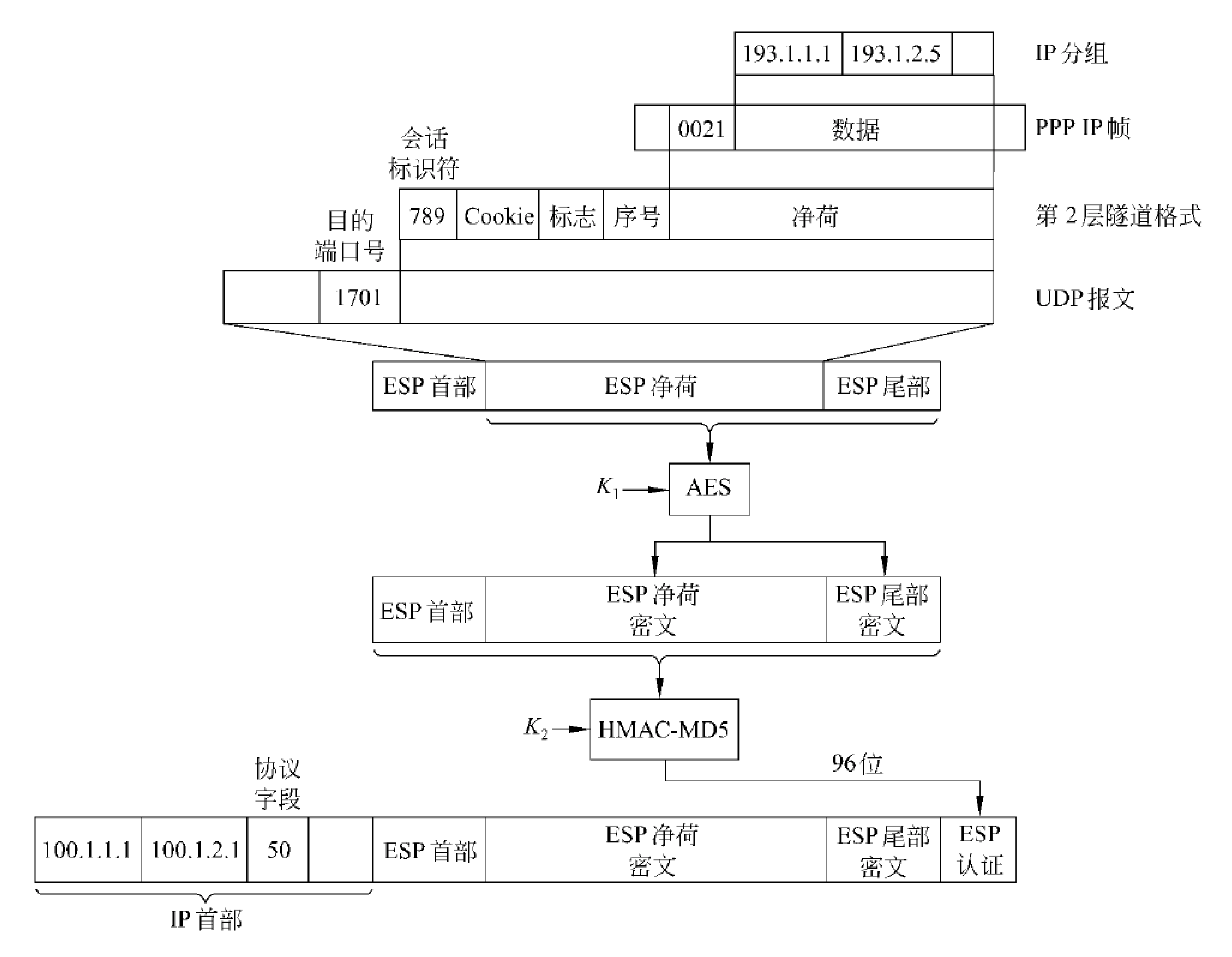


图 6.28 第 2 层隧道报文封装成 ESP 报文过程

PPP 链路建立、远程接入用户身份认证和内部网络本地 IP 地址分配等功能，将远程接入用户接入内部网络。由于建立远程接入用户和 LNS 之间第 2 层隧道的过程由远程接入用户启动，因此，将这种接入方式称为自愿隧道方式。

远程接入用户通过自愿隧道方式接入内部网络前，必须先接入 Internet，分配全球 IP 地址，然后，启动第 2 层隧道的建立过程，第 2 层隧道的两端分别是远程接入用户和 LNS。图 6.29 中的远程接入用户为了接入 Internet，完成如下过程：

(1) 建立远程接入用户和 LAC 之间的语音信道；

(2) 建立远程接入用户和 LAC 之间的 PPP 链路，并完成对远程接入用户的身份认证；

(3) LAC 为远程接入用户分配全球 IP 地址 200.1.1.1，并在路由表中添加将全球 IP 地址 200.1.1.1 和连接远程接入用户的语音信道绑定在一起的路由项。

远程接入用户接入 Internet 后，可以实现和 Internet 中其他 IP 接口的通信。在接入内部网络的过程中，LNS 相当于内部网络的网络接入服务器(NAS)，由它完成对远程接入用户的身份认证和内部网络本地 IP 地址分配，目前，最常用于实现对远程接入用户身份认证、IP 地址分配的协议是 PPP，而 PPP 是一种基于物理点对点链路的链路层协议，因此，在由 LNS 通过 PPP 实现对远程接入用户身份认证、内部网络本地 IP 地址分配前必须在远程接入用户和 LNS 之间建立点对点链路，当然，图 6.29 所示的网络结构无法在

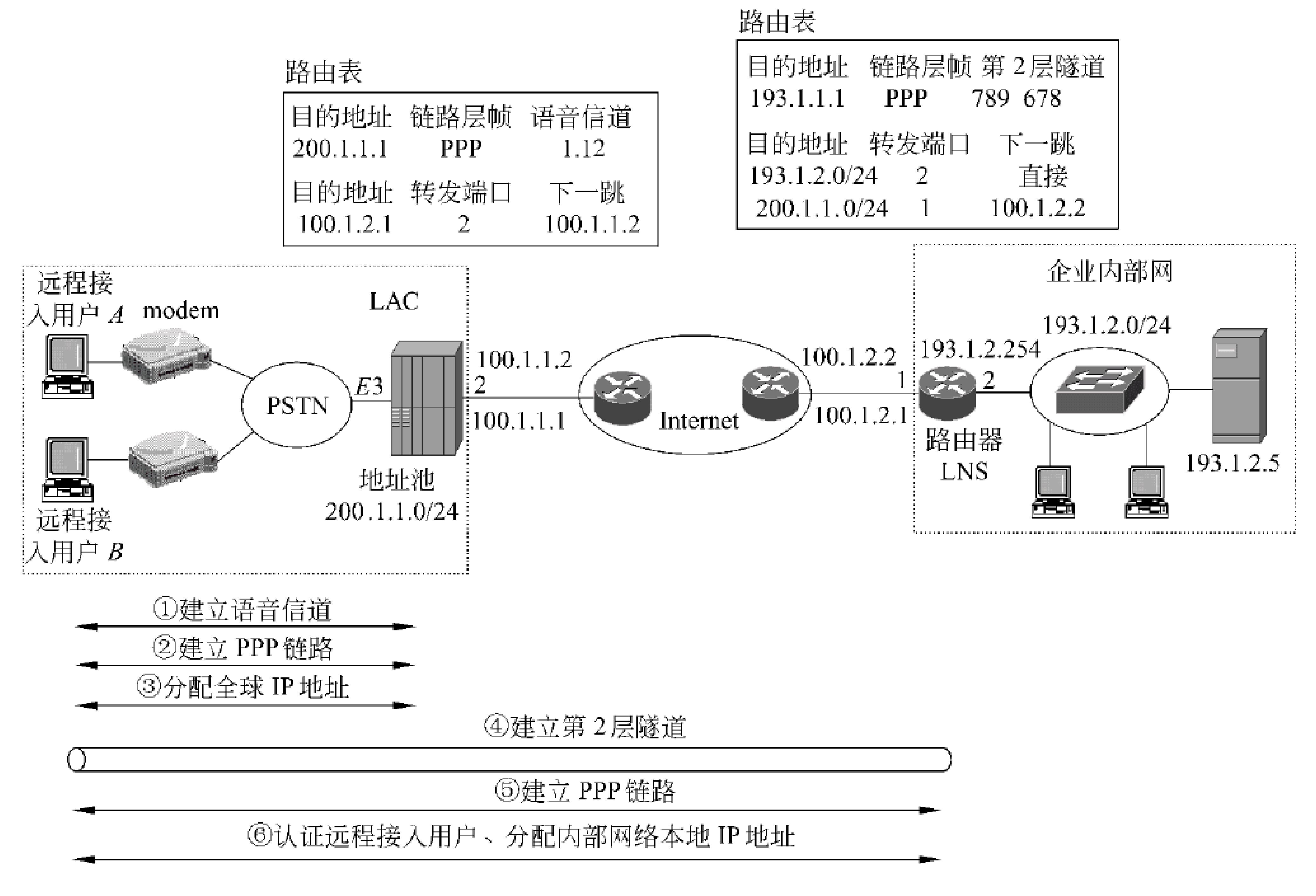


图6.29　远程接入用户自愿隧道方式接入内部网络过程

远程接入用户和LNS之间建立类似语音信道的物理点对点链路，只能通过建立基于IP网络的第2层隧道实现远程接入用户和LNS之间的PPP帧交换。LNS因此实现对远程接入用户的身份认证、内部网络本地IP地址分配，并在LNS路由表中添加将分配给远程接入用户的内部网络本地IP地址193.1.1.1和连接远程接入用户的第2层隧道绑定在一起的路由项。

2. 数据传输过程

当远程接入用户访问内部网络中的服务器时，构建以193.1.1.1为源IP地址、193.1.2.5为目的IP地址的IP分组，由于远程接入用户通过点对点虚拟线路（第2层隧道）连接内部网络的网络接入服务器（LNS），因此，该IP分组封装成PPP IP帧后，通过第2层隧道传输给LNS。

第2层隧道将PPP IP帧传输给LNS的过程如下：

(1) 将PPP IP帧封装成第2层隧道报文，第2层隧道报文以200.1.1.1为源IP地址、以100.1.2.1为目的IP地址，并通过Internet实现第2层隧道报文远程接入用户至LNS的传输过程。

(2) 远程接入用户首先将第2层隧道报文传输给ISP的接入服务器（LAC），由于远程接入用户和LAC之间用语音信道实现互连，因此，第2层隧道报文被封装成PPP IP帧后，通过语音信道传输给LAC。

(3) LAC通过连接远程接入用户的语音信道接收到PPP IP帧，从中分离出第2层

隧道报文,用第 2 层隧道报文的目的 IP 地址 100.1.2.1 检索路由表,找到下一跳路由器,将第 2 层隧道报文转发给下一跳路由器。经过 Internet 的逐跳转发,第 2 层隧道报文到达 LNS。值得指出的是:这里的 LAC 只是远程接入用户至 LNS 的第 2 层隧道报文传输路径中的一个转发结点。

LNS 接收到第 2 层隧道报文后,从中分离出 PPP IP 帧,从 PPP IP 帧中分离出 IP 分组,用 IP 分组的目的 IP 地址 193.1.2.5 检索路由表,发现服务器连接在和其直接相连的以太网上,将 IP 分组封装成 MAC 帧,通过以太网传输给服务器,完成 IP 分组远程接入用户至服务器的传输过程。远程接入用户封装 IP 分组的过程如图 6.30 所示,传输过程中各个设备的协议转换过程如图 6.31 所示。

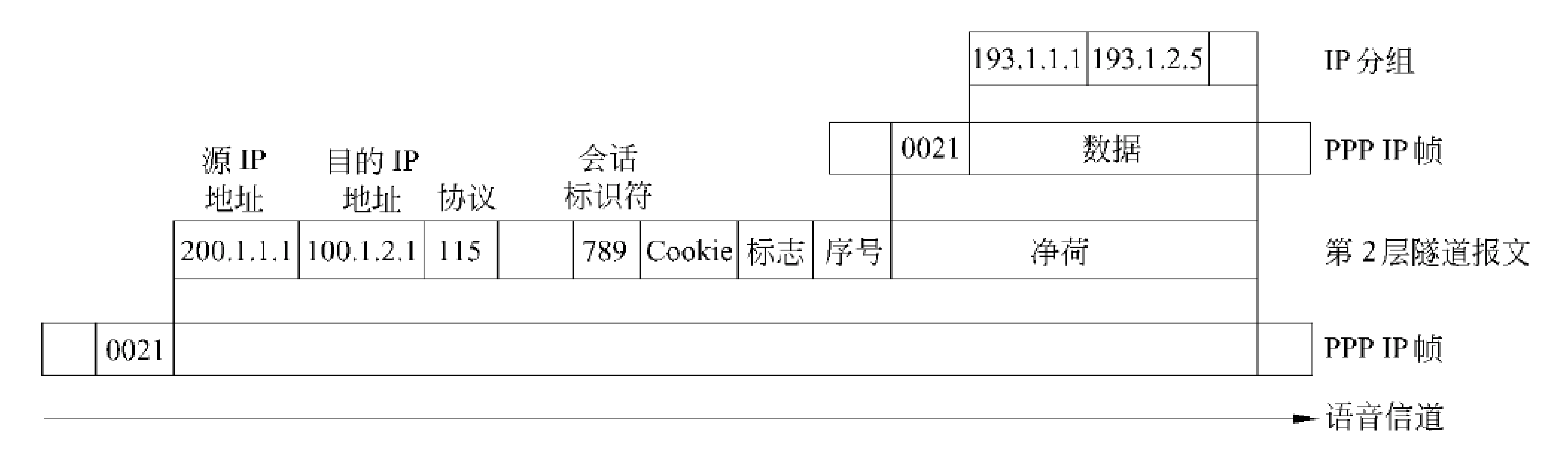


图 6.30 远程接入用户数据封装过程

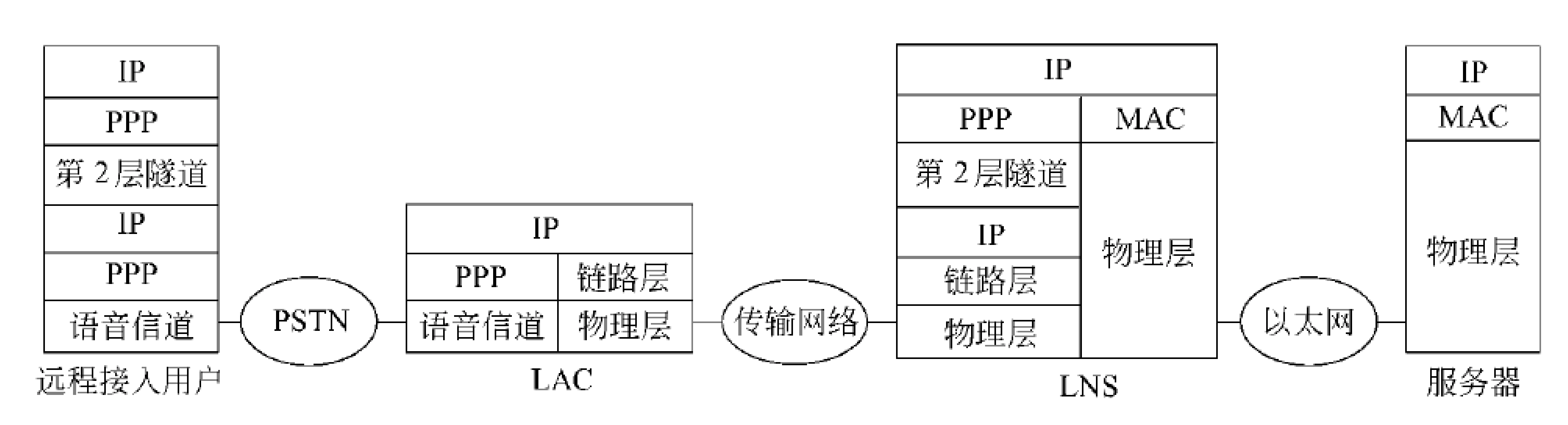


图 6.31 协议转换过程

当内部网络服务器向远程接入用户发送数据时,构建以 193.1.2.5 为源 IP 地址、193.1.1.1 为目的 IP 地址的 IP 分组,并通过以太网将 IP 分组传输给默认网关 LNS,LNS 从 MAC 帧中分离出 IP 分组,用 IP 分组的目的 IP 地址 193.1.1.1 检索路由表,找到路由项,路由项表明通过第 2 层隧道直接将 IP 分组传输给远程接入用户,将 IP 分组封装成 PPP IP 帧,然后将 PPP IP 帧封装成第 2 层隧道报文,第 2 层隧道报文的源 IP 地址为 100.1.2.1、目的 IP 地址为 200.1.1.1,将第 2 层隧道报文发送给 Internet。LNS 将第 2 层隧道报文传输给 Internet 时,作为 Internet 的边缘路由器,用第 2 层隧道报文的目的 IP 地址 200.1.1.1 检索路由表,找到 Internet 中的下一跳路由器,把第 2 层隧道报文传输给 Internet 中的下一跳路由器。第 2 层隧道报文经过 Internet 逐跳转发,到达 LNS 至远程接入用户传输路径的最后一个转发结点 LAC,LAC 用第 2 层隧道报文的目的 IP 地址 200.1.1.1 检索路由表,找到路由项,获知用语音信道连接远程接入用户,将第 2 层隧道

报文封装成 PPP IP 帧后，传输给远程接入用户，远程接入用户从 PPP IP 帧中分离出第 2 层隧道报文，从第 2 层隧道报文中分离出 PPP IP 帧，从 PPP IP 帧中分离出 IP 分组，完成 IP 分组内部网络服务器至远程接入用户的传输过程。

6.4　虚拟专用局域网服务

6.4.1　网络结构

虚拟专用局域网服务（Virtual Private LAN Service，VPLS）将多个相距甚远、用基于 IP 网络的第 2 层隧道连接的局域网作为单个局域网提供数据传输服务，网络拓扑结构如图 6.32 所示。在图 6.32 中，终端 *A* 和终端 *E* 虽然分别连接在两个通过 IP 网络互联的局域网上，但它们之间像连接在同一个局域网一样直接传输 MAC 帧。对于终端 *A* 和终端 *E* 之间的 MAC 帧传输路径，CE 作为桥设备，将从以太网端口接收到的 MAC 帧，通过第 2 层隧道转发给另一个 CE。但对于第 2 层隧道，CE 又是边缘路由器，将封装成 IP 分组的第 2 层隧道报文转发给 IP 网络中的下一跳路由器，并通过 IP 网络的逐跳转发，到达第 2 层隧道另一端的 CE。

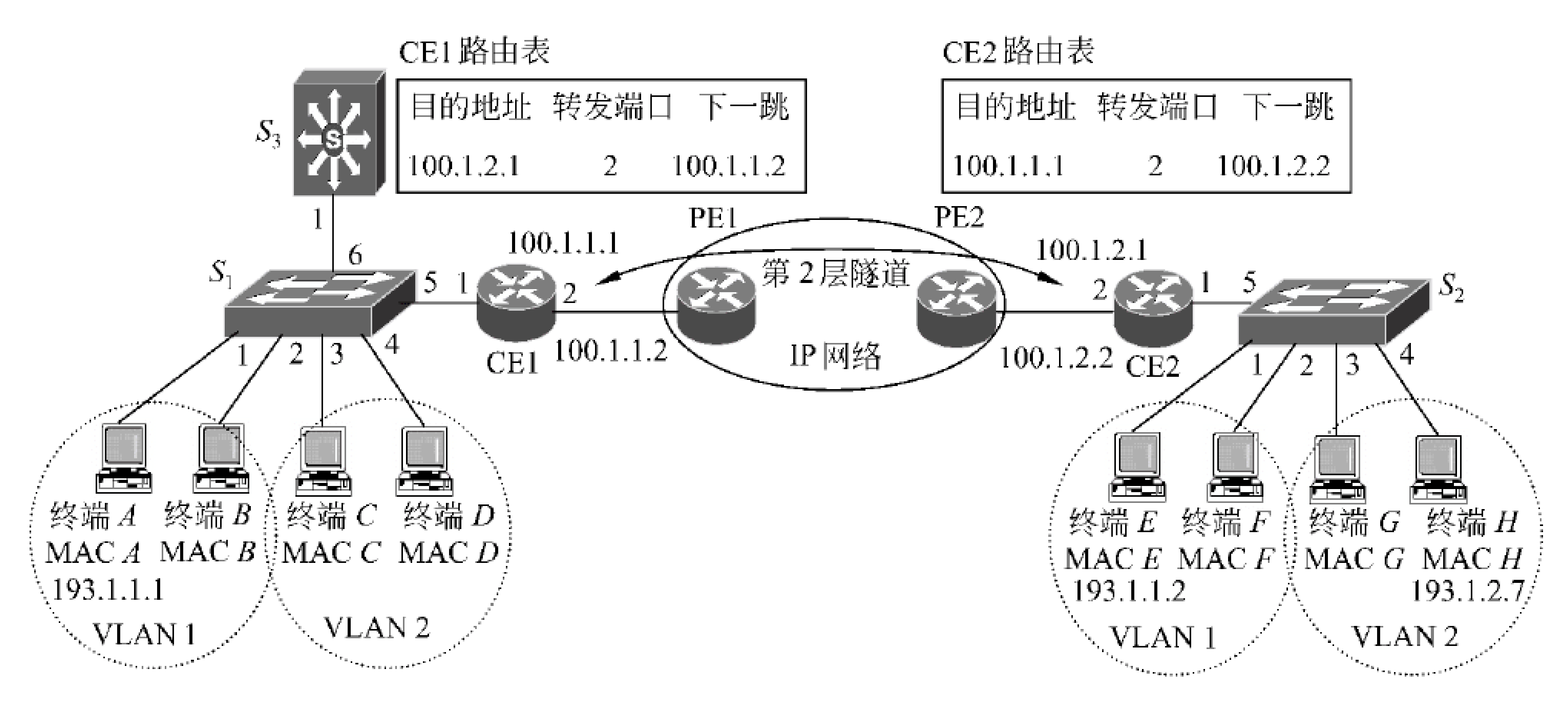


图 6.32　网络结构

在交换式以太网中，每一个 VLAN 都是独立的以太网，以太网交换机对每一个 VLAN 都有着对应的网桥和站表，以太网交换机对接收到的每一帧 MAC 帧，首先必须确定该 MAC 帧所属的 VLAN，然后，将 MAC 帧提交给所属 VLAN 对应的网桥转发。以太网交换机确定 MAC 帧所属 VLAN 的依据如下：

（1）如果 MAC 帧携带 VLAN 标识符，该 MAC 帧属于 VLAN 标识符指定的 VLAN。

（2）如果 MAC 帧没有携带 VLAN 标识符，且接收 MAC 帧的端口作为非标记端口配置了 VLAN，该 MAC 帧属于将端口作为非标记端口配置的 VLAN。

通过第 2 层隧道接收到 MAC 帧时，根据传输 MAC 帧的第 2 层隧道确定 MAC 帧所属的 VLAN，而不是 MAC 帧携带的 VLAN 标识符，因此，必须为每一个 VLAN 建立独立的第 2 层隧道，且将第 2 层隧道的会话标识符和指定的 VLAN 绑定在一起。从逻辑上

可以将每一条第 2 层隧道等同于一个非标记端口。

图 6.33 是图 6.32 对应的逻辑结构，CE 在传输 MAC 帧的过程中等同于桥设备，它和以太网交换机的不同在于需要实现传输 MAC 帧的链路的转换，将通过正常以太网链路接收到的 MAC 帧，通过第 2 层隧道发送出去，或者反之。在地址学习和转发 MAC 帧的操作中，第 2 层隧道等同于非标记端口，只是用第 2 层隧道的本地和远端会话标识符标识第 2 层隧道。CE 中必须为每一个虚拟转发实体（Virtual Forwarding Instance，VFI）绑定一条第 2 层隧道，虚拟转发实体的功能等同于网桥，只是增加了传输 MAC 帧的链路的转换功能。在 CE 中，每一个 VFI 负责一个广播域，这和每一个网桥对应一个 VLAN 是一致的，但 CE 用 VPN 标识符，而不是 VLAN 标识符标识某个广播域，因此，两个 CE 中分配相同 VPN 标识符，但不同的 VLAN 标识符的广播域是同一个广播域，由此可以看出，在 VPLS 中，VPN 标识符才是全局标识符，而 VLAN 标识符只有本地意义。在图 6.32 所示的用 IP 网络互联的两个局域网中，定义的 VLAN 只有本地意义，如果希望终端 *A* 和终端 *E* 属于同一个 VLAN，必须在 CE1 和 CE2 中为 VLAN 1 分配相同的 VPN 标识符。本例中假定 CE1 和 CE2 为 VLAN 1 和 VLAN 2 分配相同的 VPN 标识符 1 和 2。建立第 2 层隧道时，ICRQ 和 ICRP 中必须携带 VPN 标识符，第 2 层隧道两端 CE 以此将建立的第 2 层隧道和 VPN 标识符指定的 VFI 绑定在一起。图 6.34 是假定 CE1 和 CE2 之间建立控制连接的过程和图 6.23 所示一样时，分别建立和 VLAN 1、VLAN 2 对应的 VFI 绑定在一起的第 2 层隧道的过程。

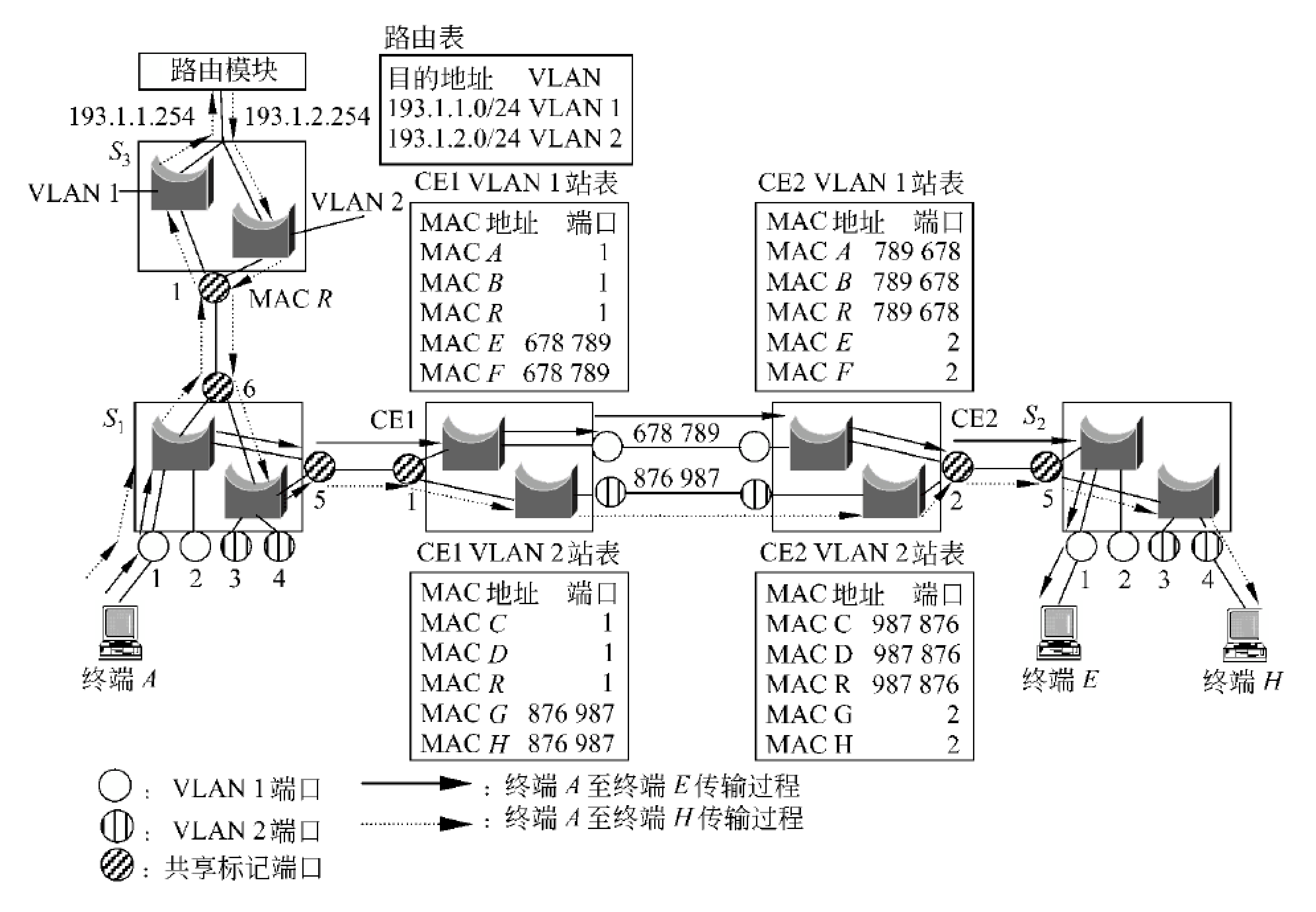


图 6.33 图 6.32 对应的逻辑结构

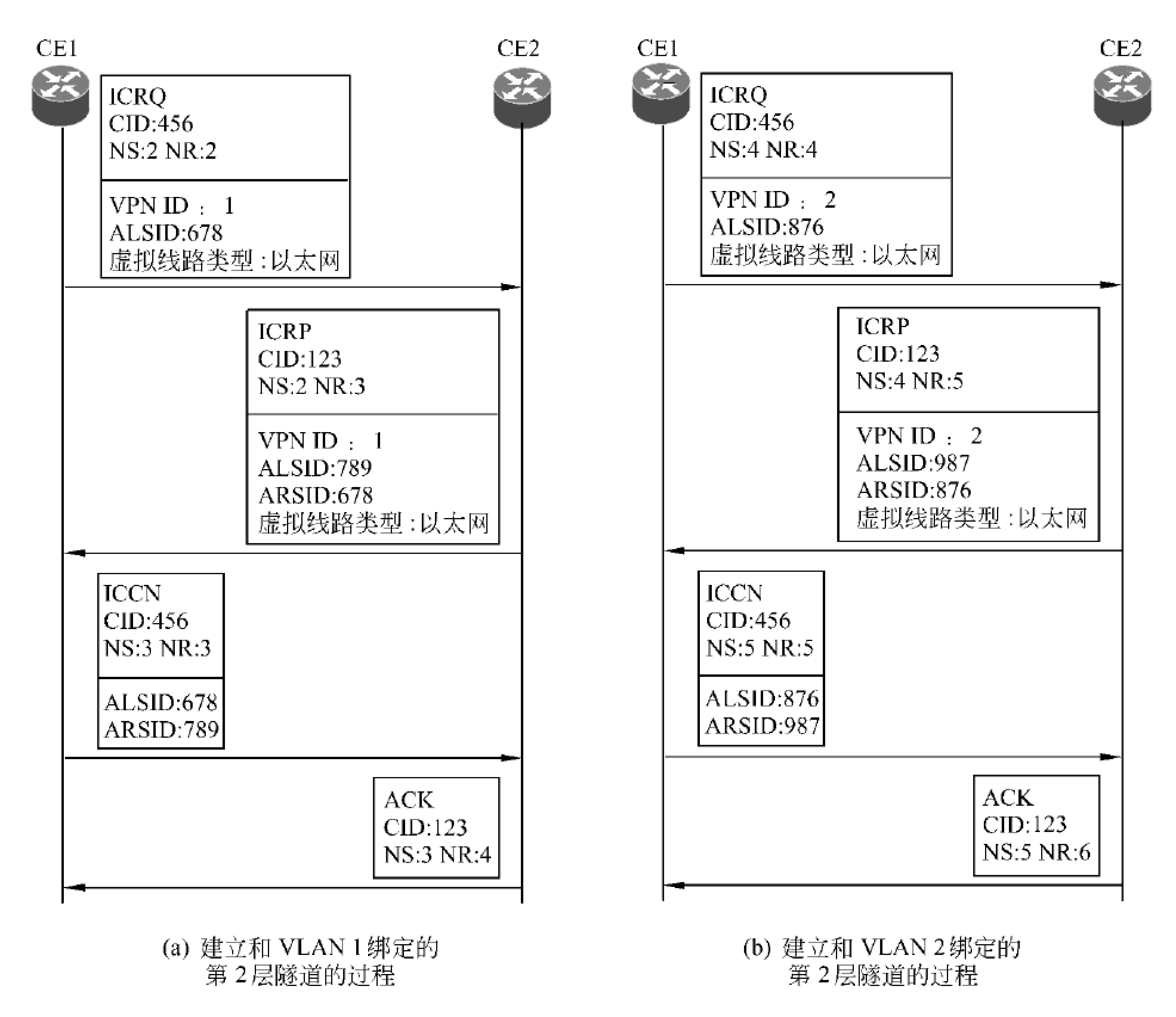


图 6.34　建立和 VLAN 绑定的第 2 层隧道的过程

6.4.2　数据传输过程

建立图 6.32 所示的逻辑结构后，可以开始局域网内终端之间的通信过程，对于以太网交换路径，CE 是一种不仅能够转发 MAC 帧，而且还能够完成 MAC 帧传输链路转换的桥设备。对于第 2 层隧道，CE 又是一个边缘路由器，负责将封装成 IP 分组的第 2 层隧道报文转发给第 2 层隧道对应的 IP 网络传输路径的下一跳路由器，并经过 IP 网络的逐跳转发到达第 2 层隧道另一端的 CE。

1. VLAN 内传输过程

当终端 A 向终端 E 传输 MAC 帧时，终端 A 构建以 MAC A 为源 MAC 地址、MAC E 为目的 MAC 地址的 MAC 帧，并将 MAC 帧发送给以太网交换机 S_1，以太网交换机 S_1 通过端口 1 接收到 MAC 帧，由于 MAC 帧没有携带 VLAN 标识符，且端口 1 是属于 VLAN 1 的非标记端口，MAC 帧被提交给 VLAN 1 对应的网桥进行转发。以太网交换机 S_1 根据 MAC 帧的目的 MAC 地址确定端口 5 为转发端口，由于端口 5 是标记端口，从端口 5 转发的 MAC 帧需要携带 VLAN ID：VLAN 1。从以太网交换机 S_1 端口 5 转发的 MAC 帧到达 CE1 端口 1，由于 CE1 端口 1 是标记端口且 MAC 帧携带 VLAN ID：

VLAN 1,MAC 帧被提交给 VLAN 1 对应的 VFI。VFI 用 MAC 帧的目的 MAC 地址检索站表,确定 MAC 帧的传输链路为第 2 层隧道,标识该第 2 层隧道的本地和远端会话标识符分别是 678 和 789。CE1 将 MAC 帧封装成第 2 层隧道报文,会话标识符为远端会话标识符 789,封装过程如图 6.35 所示。

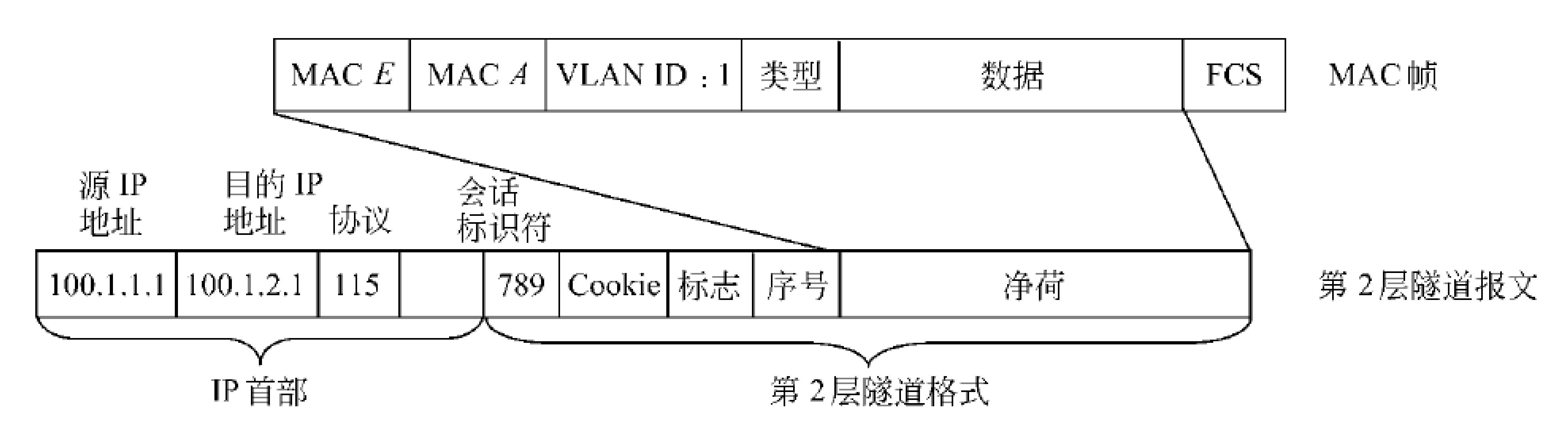


图 6.35 MAC 帧封装成第 2 层隧道报文过程

CE1 用第 2 层隧道报文的目的 IP 地址 100.1.2.1 检索路由表,找到下一跳路由器,并将第 2 层隧道报文转发给 IP 网络中的下一跳路由器,第 2 层隧道报文经过 IP 网络的逐跳转发,到达 CE2,CE2 根据传输第 2 层隧道报文的第 2 层隧道确定转发该 MAC 帧的 VFI,因此,虽然第 2 层隧道报文封装的 MAC 帧中包含 VLAN ID,但 CE2 根据第 2 层隧道报文携带的会话标识符,而不是 VLAN ID 确定转发 MAC 帧的 VFI。VFI 从第 2 层隧道报文中分离出 MAC 帧,根据 MAC 帧的目的 MAC 地址 MAC *E* 检索站表,确定端口 2 为转发端口,由于端口 2 是标记端口且转发该 MAC 帧的 VFI 和 VLAN 1 绑定,需要 MAC 帧携带 VLAN ID: VLAN 1,这里,由于 MAC 帧已经携带 VLAN ID: VLAN 1,因此,可以将 MAC 帧从端口 2 转发出去。该 MAC 帧经过交换机 S_2 转发到达终端 *E*,完成 MAC 帧终端 *A* 至终端 *E* 的传输过程。传输过程中 CE1 和 CE2 的协议转换过程如图 6.36 所示。

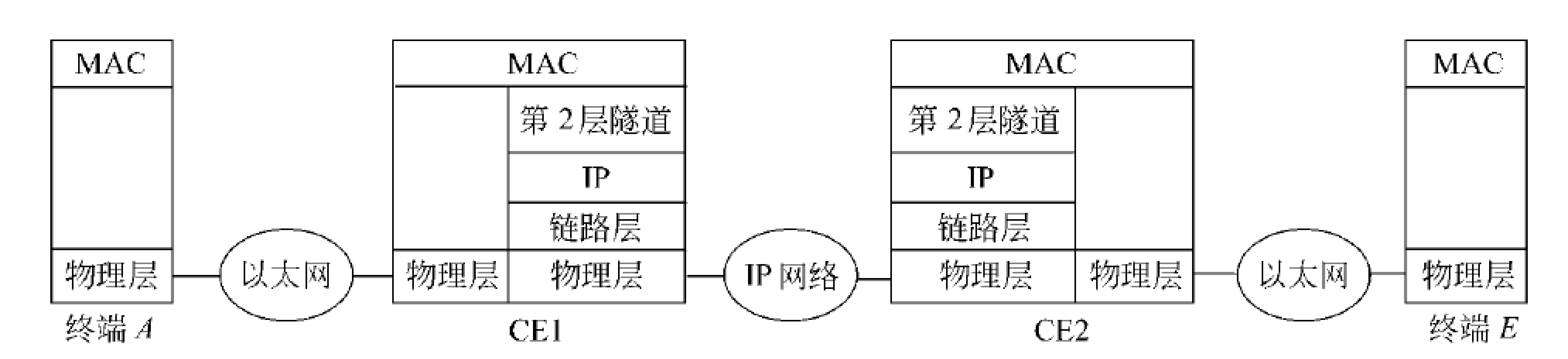


图 6.36 协议转换过程

2. VLAN 间传输过程

当终端 *A* 向终端 *H* 传输 IP 分组时,终端 *A* 构建以 193.1.1.1 为源 IP 地址、193.1.2.7 为目的 IP 地址的 IP 分组,由于源和目的 IP 地址属于不同的子网地址,因此,终端 *A* 需要将 IP 分组转发给默认网关: 三层交换机 S_3,终端 *A* 将 IP 分组封装成以 MAC *A* 为源 MAC 地址、MAC *R* 为目的 MAC 地址的 MAC 帧,通过 VLAN 1 将 MAC 帧发送给三层交换机 S_3,三层交换机 S_3 分离出 IP 分组,用 IP 分组的目的 IP 地址检索路由表,确定通过 VLAN 2 将 IP 分组发送给终端 *H*,三层交换机 S_3 将 IP 分组封装成以 MAC *R* 为源 MAC 地址、MAC *H* 为目的 MAC 地址的 MAC 帧,通过 VLAN 2 将 MAC 帧发送给终端 *H*,MAC 帧通过

VALN 2 完成三层交换机 S_3 至终端 H 的传输过程和终端 A 至终端 E 的传输过程相同，这里不再赘述，传输过程中三层交换机 S_2、CE1 和 CE2 的协议转换过程如图 6.37 所示。

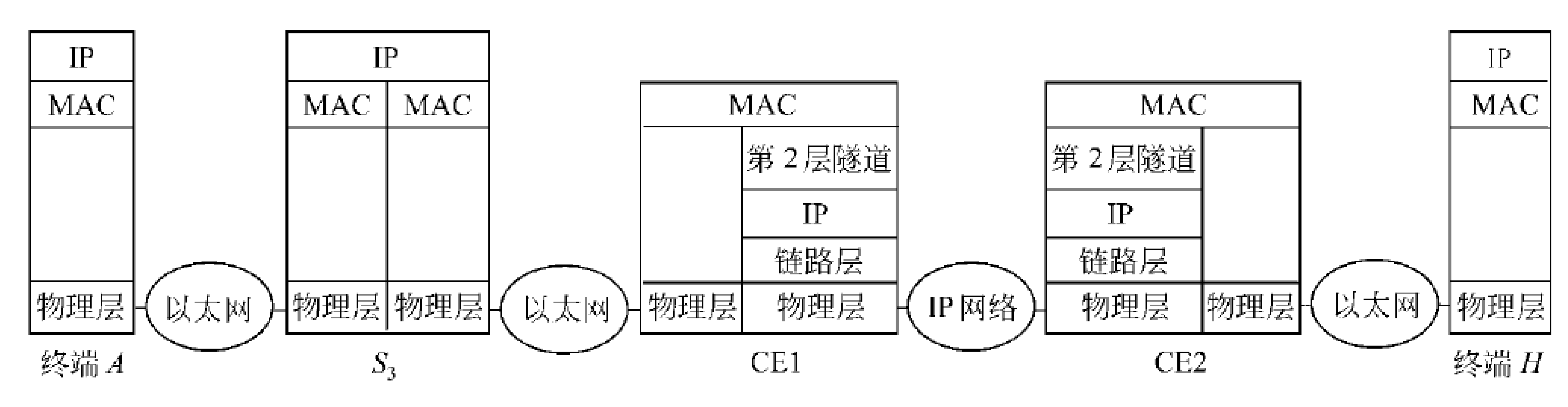


图 6.37　协议转换过程

习　　题

6.1　什么是 VPN？采用 VPN 的主要原因是什么？

6.2　目前用于实现 VPN 的技术有哪些？各有什么优缺点？

6.3　VPN 中隧道的含义是什么？和现实生活中的隧道有何异同？

6.4　如何实现隧道传输的保密性和完整性。

6.5　图 6.38 是一个 VPN 结构，分配本地 IP 地址的 LAN 1 和 LAN 2 通过 Internet 实现互联。路由器 R_1、R_2 连接 Internet 端口分配的是全球 IP 地址，给出路由器 R_1、R_2 实现 LAN 1 和 LAN 2 相互通信所需要的全部配置信息。

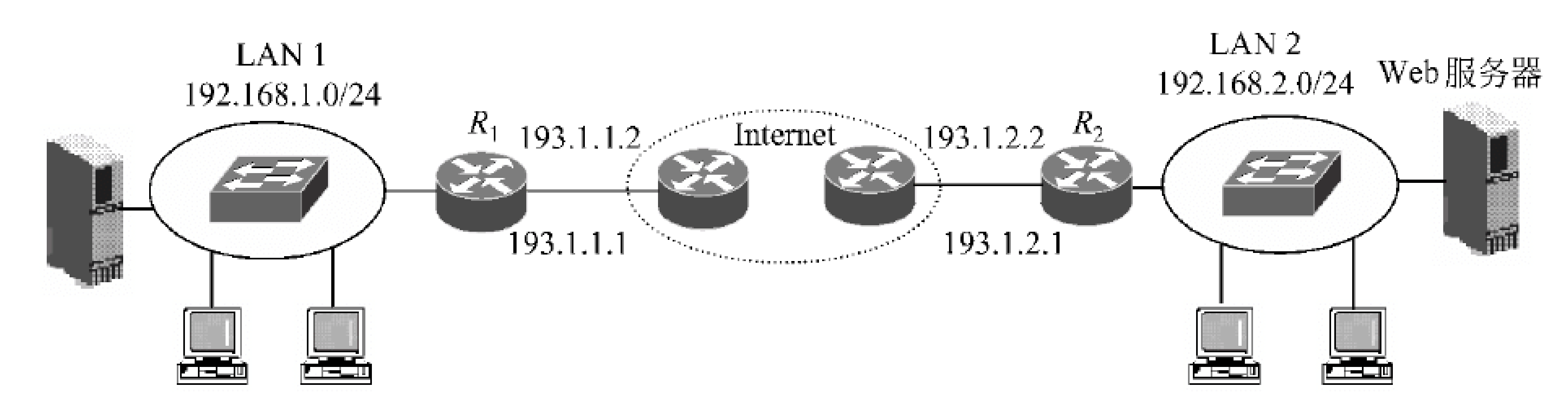


图 6.38　题 6.5～题 6.7 图

6.6　如果图 6.38 中 LAN 1 和 LAN 2 之间用 IPSec 实现安全通信，给出安全关联的静态配置信息。

6.7　如果图 6.38 中 LAN 1 和 LAN 2 之间用 IPSec 实现安全通信，且动态建立安全关联，给出相关配置信息和安全关联建立过程。

6.8　虚拟接入技术主要用来解决什么问题？

6.9　为什么说第 2 层隧道是虚拟线路？

6.10　如何理解 LAC 物理层中继设备和 Internet 边缘路由器的双重身份？

6.11　简述第 2 层隧道控制连接的作用和建立过程。

6.12　简述第 2 层隧道建立过程。

6.13　图 6.39 是一个虚拟网络结构，假定采用强制隧道方式，给出接入过程前，LAC 和 LNS 的配置信息。

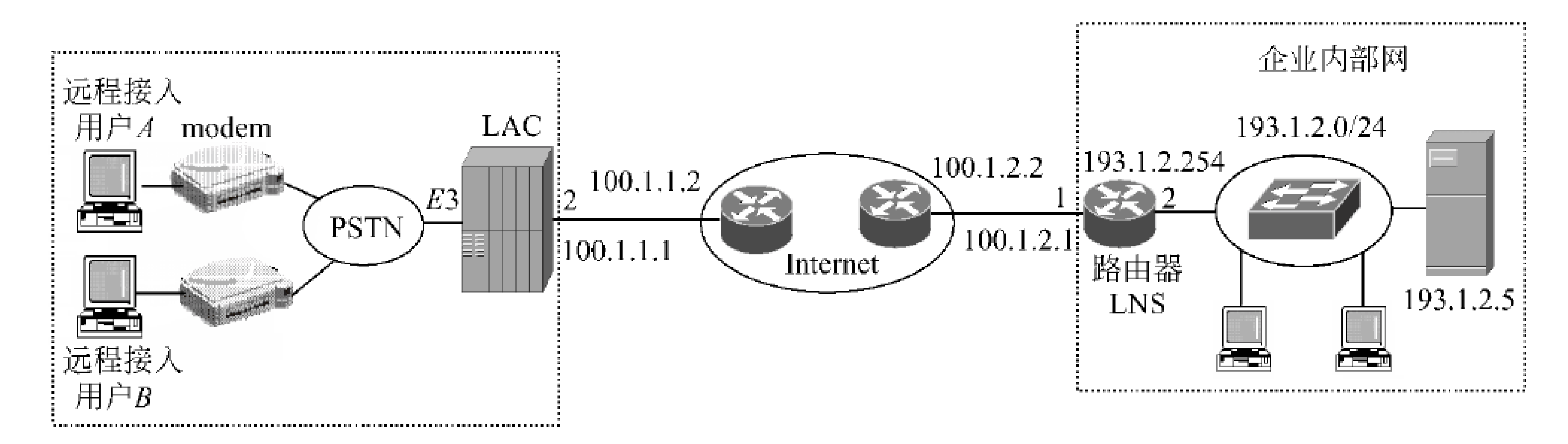


图 6.39 题 6.13～题 6.16 图

6.14 对于图 6.39 所示的网络结构，如果采用自愿隧道方式，给出接入过程前，LAC 和 LNS 的配置信息。

6.15 对于图 6.39 所示的网络结构，给出强制隧道方式下的 PPP 操作过程。

6.16 对于图 6.39 所示的网络结构，给出自愿隧道方式下的 PPP 操作过程。

6.17 如何理解图 6.40 中路由器 CE 网桥和 Internet 边缘路由器的双重身份？

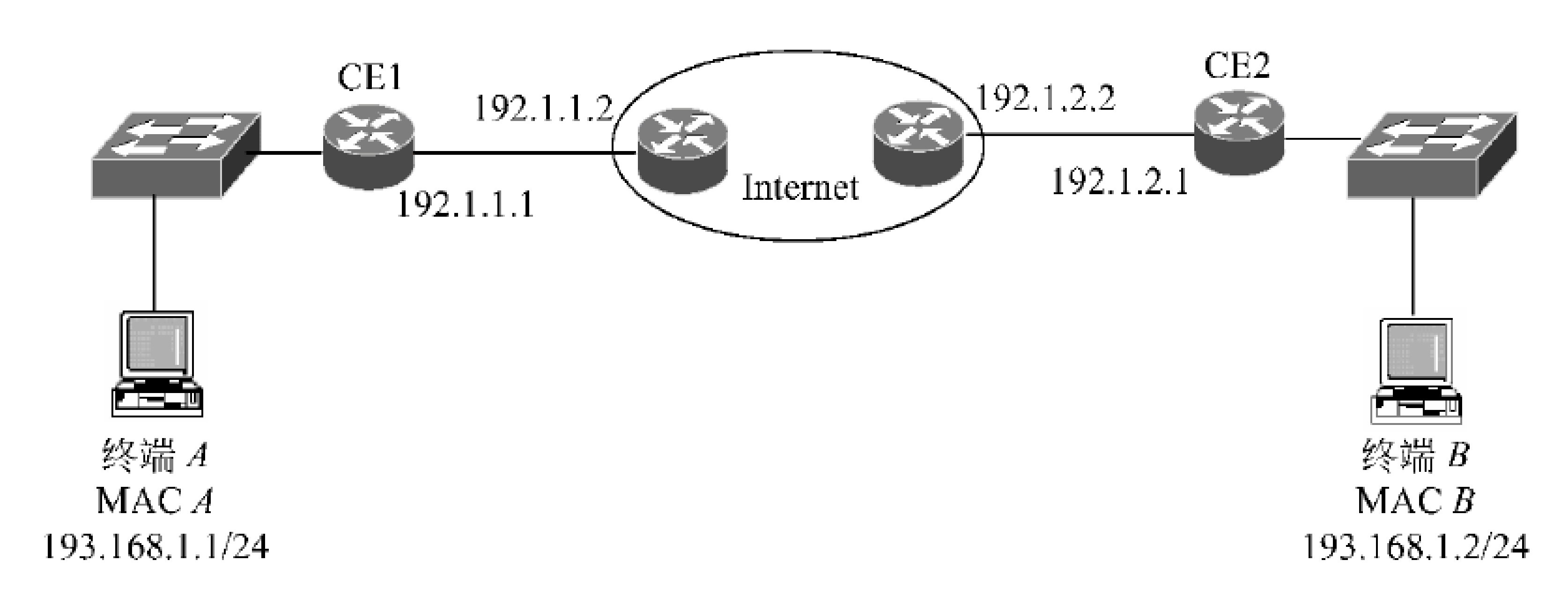


图 6.40 题 6.17～题 6.20 图

6.18 根据图 6.40 所示的网络结构，给出 CE1 和 CE2 作为网桥和 Internet 边缘路由器的配置信息。

6.19 根据图 6.40 所示的网络结构，给出终端 *A* 用 ARP 解析终端 *B* MAC 地址的过程。

6.20 根据图 6.40 所示的网络结构，给出终端 *A* 向终端 *B* 发送 MAC 帧的过程。

6.21 网络结构如图 6.41 所示，企业内部网络分配本地 IP 地址，远程接入用户如何通过 VPN 像企业内部网络中的本地终端一样访问企业内部网络资源，给出实现这一功能所要求的配置信息和远程接入用户访问内部网络资源的过程。

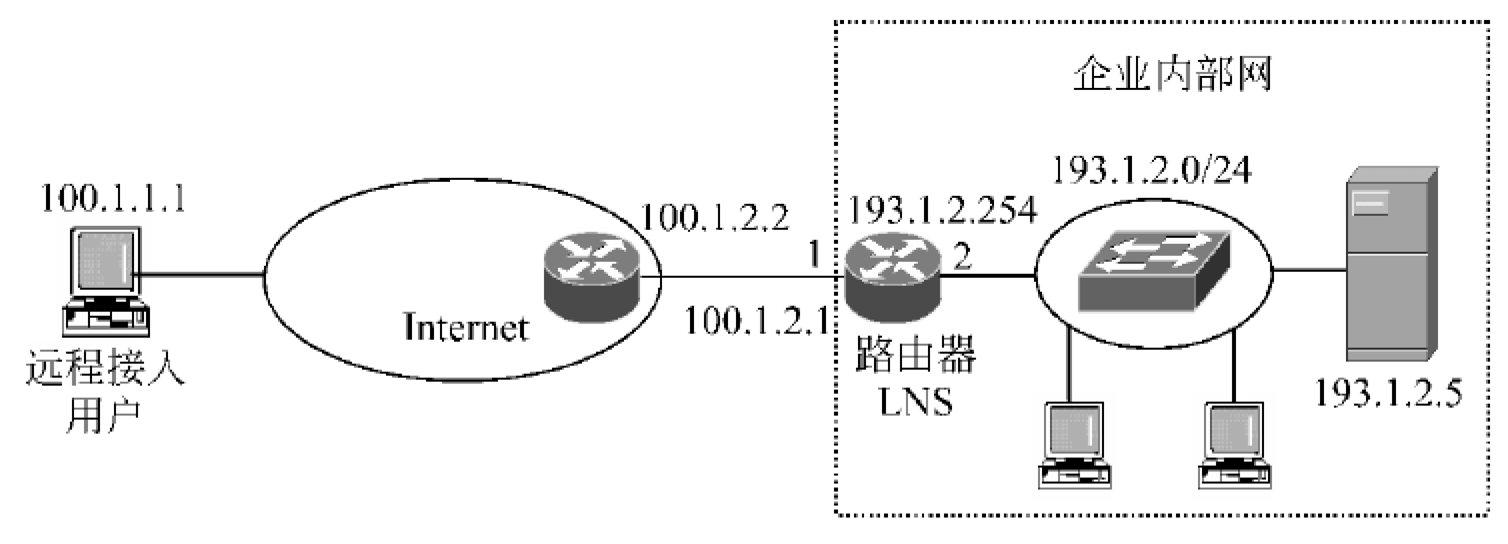


图 6.41 题 6.21 图

第7章 防火墙

CHAPTER

随着网络应用的普及，网络开始面临这样的窘境：一方面为了实现信息共享，必须实现网络互联，并允许各子网间相互交换信息。另一方面为了信息安全，必须对信息访问过程实施严格控制。这就需要一种新的互连设备，它一方面允许子网间必要的信息交换，另一方面通过制定访问控制策略，对子网间信息传输过程实施严格控制，这种新型互连设备就是防火墙。

7.1 防火墙概述

7.1.1 防火墙功能

防火墙功能主要包括服务控制、方向控制、用户控制和行为控制。

1. 服务控制

网络中大量信息流和服务有关，如 Web 服务、FTP 服务产生的信息流，所谓服务控制就是通过制定相应的安全策略只允许子网间相互交换和特定服务相关的信息，这就要求防火墙具有从信息流中鉴别出和特定服务有关的信息的能力。

2. 方向控制

防火墙通过制定相应的安全策略不仅可以将允许子网间相互交换的信息限制为和特定服务相关的信息，而且可以限制该特定服务的发起端，即只允许子网间相互交换和由属于某个特定子网的终端发起的特定服务相关的信息。

3. 用户控制

防火墙通过制定相应安全策略设定每一个用户的访问权限，对每一个访问网络资源的用户进行认证，并根据认证结果确定该用户本次访问的合法性，从而实现对每一个用户的访问过程的控制。

4. 行为控制

防火墙通过制定相应安全策略对访问网络资源的行为进行控制，如过滤垃圾邮件，防止 SYN 泛洪攻击等，假定防火墙安全策略允许正常的邮件

服务和 TCP 连接建立过程，但可以对这些服务的行为予以限制，如禁止某些地址发送的或具有不正当内容的邮件继续传输，限制特定服务器每秒内尚未完成的 TCP 连接数等，通过这些行为限制，预防和阻止黑客攻击。

7.1.2 防火墙分类

防火墙分类如图 7.1 所示，根据所作用的范围可以将防火墙分为个人防火墙和网络防火墙。

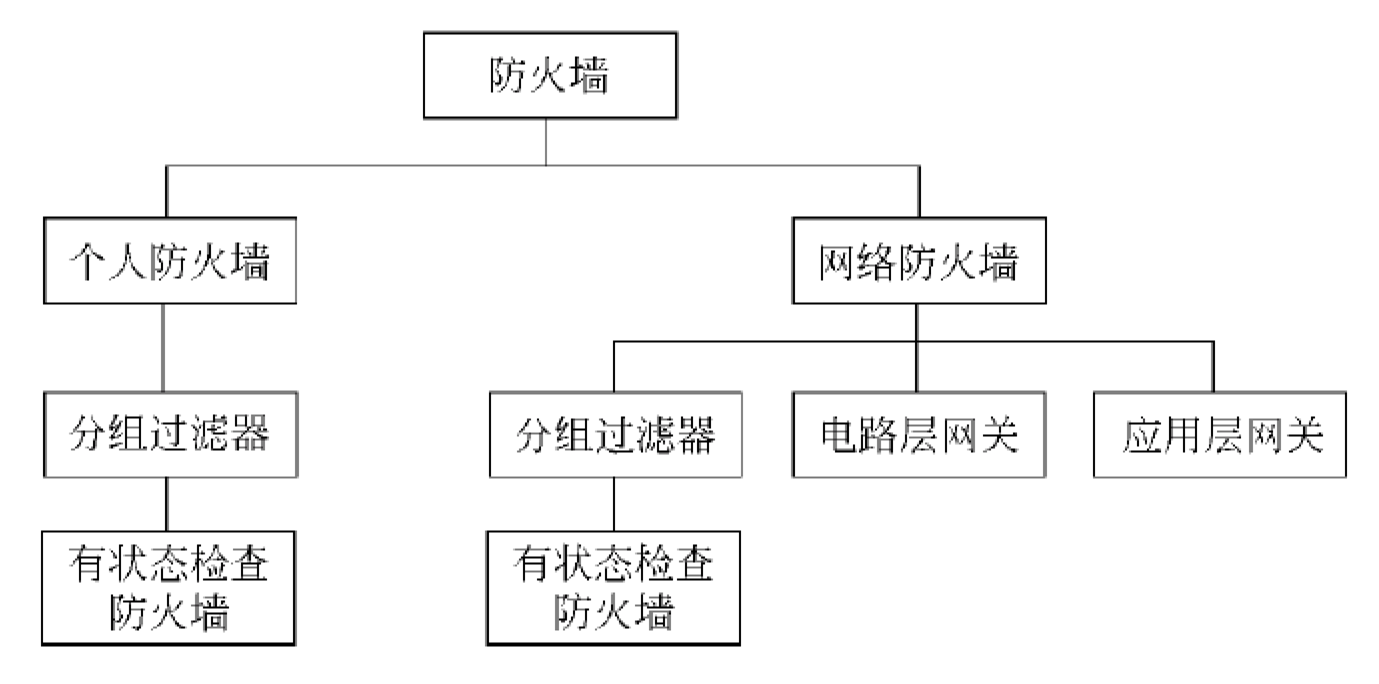


图 7.1 防火墙分类

1. 个人防火墙

个人防火墙只保护单台计算机，用于对进出计算机的信息流实施控制，因此，个人防火墙通常是分组过滤器，能够根据用户制定的安全策略监测进出计算机的 IP 分组，过滤掉安全策略不允许传输的 IP 分组。

分组过滤器分为有状态和无状态两种类型，无状态分组过滤器只根据单个 IP 分组携带的信息确定是否过滤掉该 IP 分组，而有状态分组过滤器不仅根据 IP 分组携带的信息，而且还根据 IP 分组所属的会话状态确定是否过滤掉该 IP 分组。

传统个人防火墙的分组过滤功能只是网络防火墙类型中分组过滤器的子集，但目前一些个人防火墙将分组过滤功能和操作系统中的安全访问功能相结合，提供了一些数据安全访问功能，而且可以基于文件实施安全访问策略，因此，个人防火墙在保护数据安全性，防止黑客攻击和病毒感染方面，有着网络防火墙不可替代的优势，但对于企业网中成千上万台计算机，不仅无法承受为每一台计算机安装个人防火墙所需要的费用，更无法对计算机配置统一的安全策略。因此，个人防火墙更多用于家庭用计算机。

2. 网络防火墙

网络防火墙通常位于内网和外网之间的连接点，对内网中的信息资源实施保护，目前作为网络防火墙的主要有分组过滤器（分为无状态和有状态两种）、电路层网关和应用层网关。

1）分组过滤器

分组过滤器根据用户制定的安全策略对内网和外网间传输的信息实施控制，它对信息的发送端和接收端是透明的，因此，分组过滤器的存在无须改变终端访问网络的方式。随着有状态分组过滤器的应用，防火墙对内网和外网间传输的信息流的监控变得更加精致，因此，分组过滤器是目前应用最广泛的通用网络防火墙。

2）电路层网关

图 7.2 给出了一个典型的电路层网关的工作机制，终端发送的用于和某个服务器建立 TCP 连接的请求报文被电路层网关截获，由电路层网关向终端发送同意建立 TCP 连接的响应报文，并在接收到终端发送的确认报文后，向终端推送一个用于认证用户的 Web 页面，要求终端用户输入用户名和口令，并在用户名和口令验证无误的情况下，向服务器转发终端发送的建立 TCP 连接的请求报文，并建立电路层网关和服务器之间的 TCP 连接。从图 7.2 可以看出，终端和服务器之间的 TCP 连接由终端和电路层网关之间的 TCP 连接和电路层网关和服务器之间的 TCP 连接组成，终端和服务器之间交换的信息经过电路层网关中继，电路层网关在运输层对信息的合法性进行检测，如 IP 分组是否属于某个合法的 TCP 连接，序号和确认序号是否合理等。

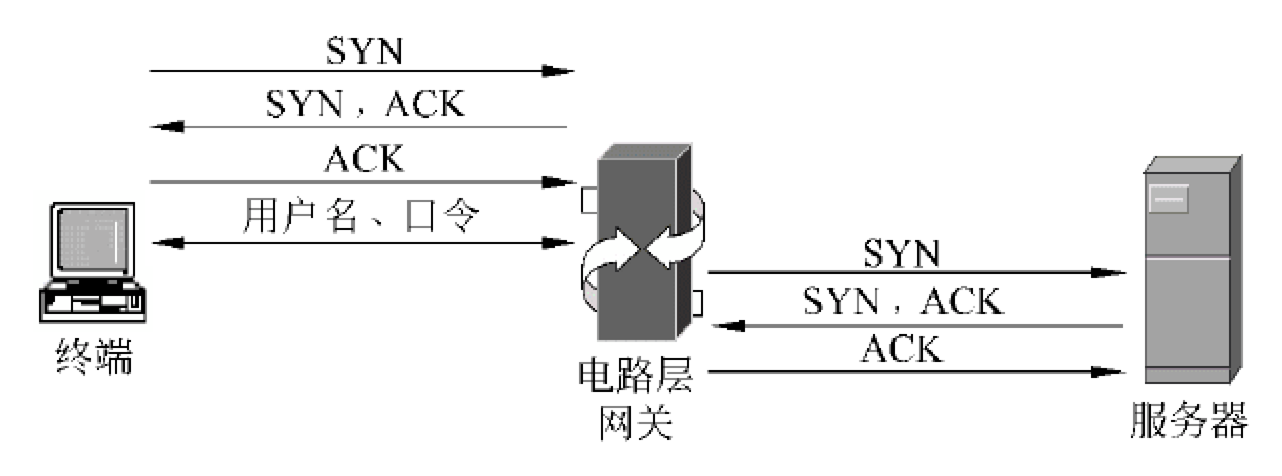


图 7.2　电路层网关工作机制

电路层网关对终端可以是透明的，也可以是不透明的，如果是不透明的，电路层网关就是一个代理，终端需要同时给出代理和服务器的 IP 地址（或是完全合格的域名），终端先和代理建立 TCP 连接，代理在完成对终端用户的身份认证后，和服务器建立 TCP 连接，并将这两个 TCP 连接绑定在一起。如果电路层网关对终端是透明的，终端和服务器之间的传输通路必须经过电路层网关，电路层网关能够截获终端发送给服务器的请求建立 TCP 连接的请求报文。

3）应用层网关

应用层网关的工作机制和电路层网关相似，但电路层网关一般只在运输层检测相互交换的信息的合理性，而应用层网关在应用层对相互交换的信息的合理性进行检测，图 7.3 给出了终端用 FTP 从文件服务器下载文件的操作过程。如果是电路层网关，它在中继终端发送的 FTP 请求报文和文件服务器发送的 FTP 响应报文时，只对报文所属的 TCP 连接，及报文携带的序号和确认序号的合理性进行检测，因此，电路层网关是应用层无关的，它适用于所有应用层协议。如果是应用层网关，对相互交换的 FTP 报文，必须根据 FTP 规范检测其合



图 7.3　终端通过 FTP 下载文件的操作过程

理性，包括请求和响应报文中的参数是否正确？请求报文和响应报文是否匹配？文件内容是否包含禁止传播的非法内容或病毒等。应用层网关必须支持 FTP，才能中继 FTP 报文，因此，应用层网关是应用层相关的。和电路层网关一样，应用层网关对终端可以是透明的，也可以是不透明的。

随着网络防火墙的发展，这种分类越来越模糊，目前的网络防火墙往往是综合了多种类型的防火墙功能的综合防火墙。

7.2 分组过滤器

分组过滤器分为无状态和有状态两种类型，无状态分组过滤器基于单个 IP 分组进行操作，每一个 IP 分组都是独立的个体。有状态分组过滤器基于会话进行操作，对每一个 IP 分组，不仅需要根据 IP 分组自身属性，而且还需根据会话状态确定对其的操作。

7.2.1 无状态分组过滤器

无状态分组过滤器通过规则从 IP 分组流中鉴别出一组 IP 分组，然后对其实施规定的操作，通常情况下，实施的操作有正常转发和丢弃。

规则由一组属性值组成，如果某个 IP 分组携带的信息和构成规则的一组属性值匹配，意味着该 IP 分组和该规则匹配，对该 IP 分组实施相关操作：正常转发或丢弃。

构成规则的属性值通常由下述信息组成：

- 源 IP 地址，用于匹配 IP 分组 IP 首部中的源 IP 地址字段值。
- 目的 IP 地址，用于匹配 IP 分组 IP 首部中的目的 IP 地址字段值。
- 源和目的端口号，用于匹配作为 IP 分组净荷的运输层报文首部中源和目的端口号字段值。
- 协议类型，用于匹配 IP 分组 IP 首部中的协议字段值。

无状态分组过滤器可以作用于端口的输入或输出方向，如果作用于输入方向，每一个输入 IP 分组都和过滤器中的规则进行匹配操作，如果和某个规则匹配，则对其进行过滤器规定的操作，如果实施的操作是丢弃，不再对该 IP 分组进行后续的转发处理。一个过滤器可以由多个规则构成，IP 分组只有和当前规则不匹配时，才继续和后续规则进行匹配操作，一旦和某个规则匹配，则对其进行过滤器规定的操作，不再和其他规则进行匹配操作，因此，IP 分组和规则的匹配操作顺序直接影响该 IP 分组所匹配的规则，也因此确定了对该 IP 分组实施的操作。如果过滤器作用于输出方向，则只有当该 IP 分组确定从该端口输出时，才将该 IP 分组和过滤器中的规则进行匹配操作。

下面通过一个实例来讨论确定构成规则的一组属性值的过程。在图 7.4 所示的网络中，假定要求子网 193.1.1.0/24 中终端不允许用 Telnet 访问子网 193.1.2.0/24 中服务器(193.1.2.5)，可以用分组过滤技术实现这一目标。

如果不希望 LAN 1 中终端用 Telnet 方式访问 LAN 2 中服务器，可以在路由器 R_1 的端口 1 的输入方向上设置过滤器，过滤掉所有和 LAN 1 中终端用 Telnet 访问 LAN 2 中服务器的操作关联的 IP 分组。那么，这些 IP 分组有什么特征呢？第一，这些进入路由

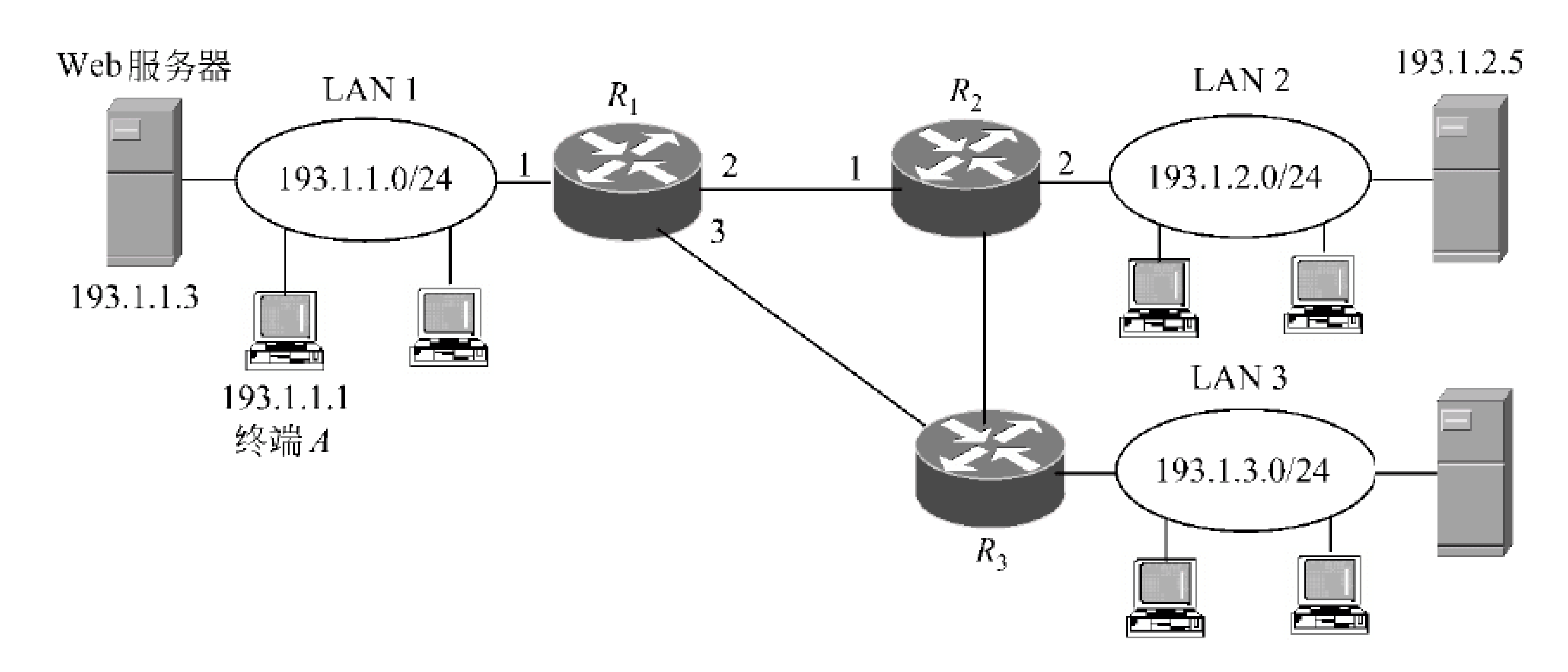


图 7.4　网络结构

器 R_1 的端口 1 的 IP 分组的源 IP 地址必须属于为 LAN 1 分配的子网地址，即源 IP 地址属于 193.1.1.0/24(193.1.1.0～193.1.1.255)。第二，其目的 IP 地址必须是 LAN 2 中服务器地址：193.1.2.5。但光有这两项只能证明 IP 分组是 LAN 1 中终端发送给 LAN 2 中服务器的 IP 分组，不能证明这些 IP 分组是和 LAN 1 中终端用 Telnet 访问 LAN 2 中服务器的操作关联的 IP 分组，如何进一步从 LAN 1 中终端发送给 LAN 2 中服务器的 IP 分组中提取出和用 Telnet 访问 LAN 2 中服务器的操作关联的 IP 分组呢？这就需要了解 LAN 1 中终端用 Telnet 访问 LAN 2 中服务器的机制。LAN 1 中终端在用 Telnet 访问 LAN 2 中服务器之前，必须先和 LAN 2 中服务器建立 TCP 连接，建立 TCP 连接时选择的源端口号是随机的，但目的端口号是固定的，为 23。因此，LAN 1 内终端发送的无论用于请求建立 TCP 连接的 TCP 请求报文，还是用于传输用 Telnet 访问 LAN 2 内服务器所要求的命令和数据的 TCP 数据报文，它的目的端口号都是 23，只要过滤掉了源 IP 地址属于 193.1.1.0/24，目的 IP 地址＝193.1.2.5，目的端口号＝23 的 IP 分组，就可以阻止 LAN 1 内终端用 Telnet 访问 LAN 2 内服务器，因此，路由器 R_1 端口 1 输入方向上的分组过滤器的规则应该是：

源 IP 地址＝193.1.1.0/24 .and. 目的 IP 地址＝193.1.2.5/32 .and. 目的端口号＝23，对和规则匹配的 IP 分组采取的动作是：丢弃。

规则中源 IP 地址＝193.1.1.0/24 的条件，是指只要 IP 分组的源 IP 地址的前 24 位＝193.1.1，则上述等式成立，这就意味着 193.1.1.0～193.1.1.255 都等于 193.1.1.0/24。而规则中目的 IP 地址＝193.1.2.5/32 的条件，意味着只有 32 位目的 IP 地址＝193.1.2.5 的IP 分组才符合上述等式。

如果为路由器 R_1 端口 1 的输入方向上设置的过滤器只是需要过滤掉所有和 LAN 1 中终端用 Telnet 访问 LAN 2 中服务器的操作关联的 IP 分组，允许其他 IP 分组继续传输，则完整的过滤器如下：

(1) 源 IP 地址＝193.1.1.0/24 .and. 目的 IP 地址＝193.1.2.5/32 .and. 目的端口号＝23，丢弃。

(2) 源 IP 地址＝0.0.0.0 .and. 目的 IP 地址＝0.0.0.0 .and. 源端口号＝ * .and. 目的端口号＝ * ，正常转发。

所有和 LAN 1 中终端用 Telnet 访问 LAN 2 中服务器的操作关联的 IP 分组和规则(1)匹配，执行丢弃操作，其他和规则(1)不匹配的 IP 分组，和规则(2)匹配，正常转发。规则(2)中的 0.0.0.0 表示任意 IP 地址，* 表示任意端口号，因此，规则(2)和所有 IP 分组匹配。从上述讨论中可以看出 IP 分组进行匹配操作的规则的顺序对 IP 分组操作结果的影响，如果 IP 分组先和规则(2)进行匹配操作，则所有 IP 分组，包括和 LAN 1 中终端用 Telnet 访问 LAN 2 中服务器的操作关联的 IP 分组都正常转发。

分组过滤是一种比较容易理解的控制信息流动的技术，但这种技术对解决一些复杂的信息流控制功能就显得有些困难了。

假定只允许 LAN 2 内终端访问 LAN 1 内的 Web 服务器，不允许 LAN 1 内终端访问 LAN 2 内的任何资源。这就意味着只有和 LAN 2 内终端发起的、对 LAN 1 内 Web 服务器访问相关的信息流才能从 LAN 1 进入 LAN 2。读者或许想到可以用分组过滤的办法来解决这一问题，在路由器 R_2 的端口 2 的输出方向设置一过滤器，过滤器的规则如下：

源 IP 地址＝193.1.1.3/32 .and. 目的 IP 地址＝193.1.2.0/24 .and. 源端口号＝80，对和规则匹配的 IP 分组采取的动作是：正常转发。

但设置这样的过滤器会带来一些问题，一是过滤器必须有其他规则和响应动作表明来自 LAN 1 的 IP 分组中只有满足了上述规则的 IP 分组才允许进入 LAN 2，其余来自 LAN 1 的 IP 分组都应该过滤掉，而其他来自别的子网且允许进入 LAN 2 内的 IP 分组仍然允许进入 LAN 2 内(LAN 2 内终端需要和其他网络内的终端通信)。二是符合上述规则的 IP 分组未必就是和 LAN 2 内终端发起的、访问 LAN 1 内 Web 服务器的操作有关的 IP 分组。如果 LAN 1 内终端 A 想攻击 LAN 2 内服务器，它可以将自己的 IP 地址从 193.1.1.1 变为 193.1.1.3，另外，通过自己编制 Telnet 访问程序，使自己的源端口号＝80，这种情况下，LAN 1 内终端 A 通过 Telnet 访问 LAN 2 内服务器的 IP 分组也能满足在路由器 R_2 端口 2 输出方向上设置的过滤器，使得 LAN 1 内终端 A 能够成功实施对 LAN 2 内服务器的攻击，因此，简单的分组过滤技术不能有效地限制子网间信息的流动。

7.2.2 有状态分组过滤器

1. 有状态分组过滤器实现原理

一般由专用防火墙提供有状态分组过滤器功能。为了实施有状态分组过滤器功能，首先需要把网络分成多个区，每一个区由一个或多个子网组成，由于专用防火墙的每一个端口可以定义成多个不同的接口，这些接口可以连接不同的子网，因此，专用防火墙的多个不同的端口可以属于同一个区，同一个端口可以属于多个不同的区。有状态分组过滤器通过访问控制策略控制区之间的信息流动。图 7.5 是一般企业网的结构，这种网络结构通常由三个区组成：信任区是企业内部网，只允许企业内部人员对其进行访问。非军事区(Demilitarized Zone，DMZ)主要由企业对外公开的服务器群组成，如 Web 服务器、电子邮件服务器等。非信任区主要指外部网络，如 Internet。一般的访问控制策略是：企业内部人员允许访问非军事区中的服务器，还可以对 Web 服务器进行管理，如修改主页

等。从使用方便性出发,企业内部人员应该允许任意访问外部网络,但为了保证内部网络的安全,同时也避免类似 P2P 这样的应用大肆占用网络带宽的情况发生,对企业内部人员访问外部网络也进行限制。外部网络只允许访问非军事区中的服务器,不允许访问企业内部网。有状态分组过滤器实现这一安全访问策略的过程如下。

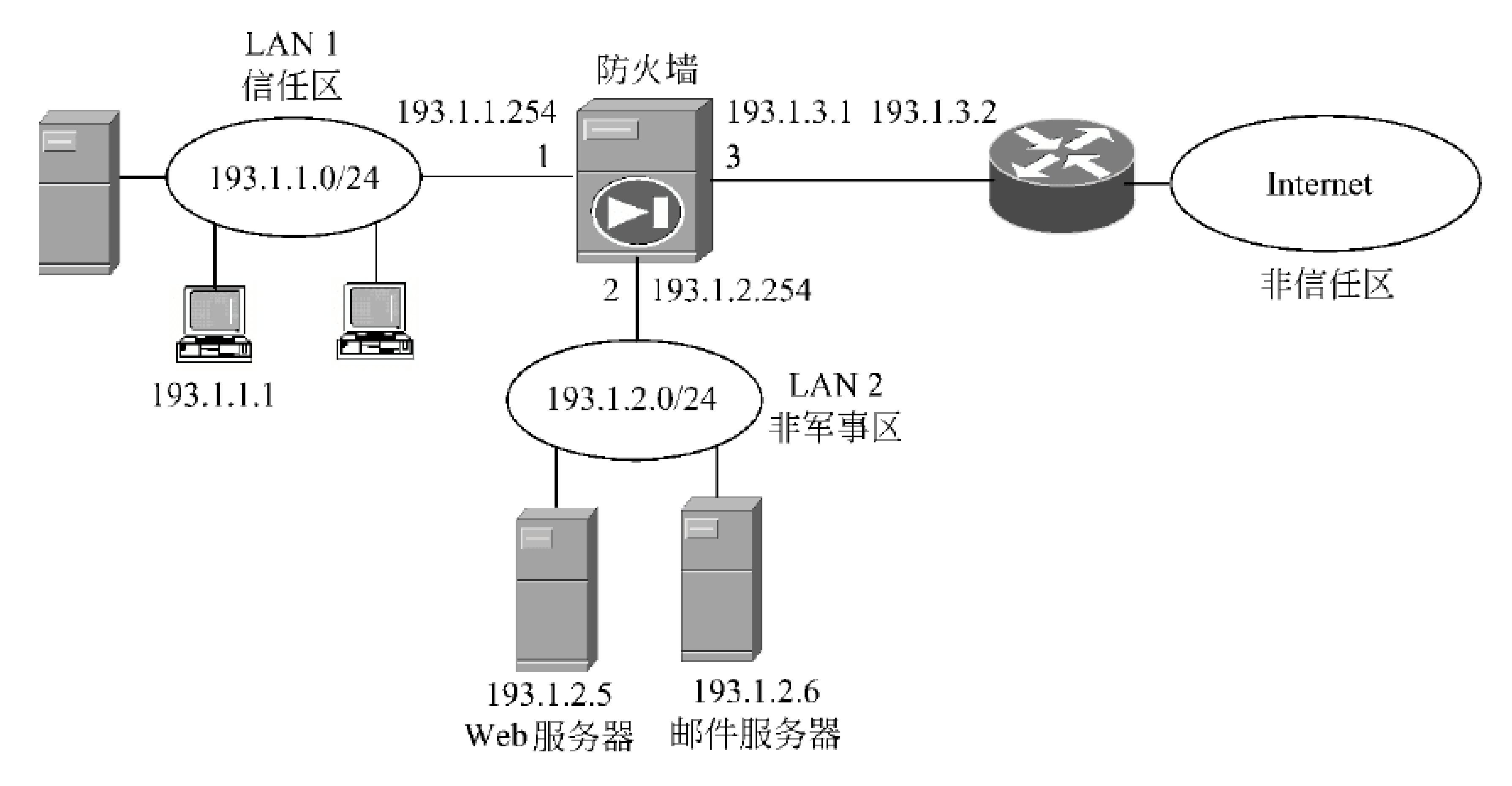


图 7.5　防火墙控制区之间信息流动

(1) 将网络分成信任区、非军事区(DMZ)、非信任区三个区,然后将防火墙的三个端口和这三个区绑定在一起,端口 1 绑定信任区,端口 2 绑定非军事区(DMZ),端口 3 绑定非信任区。

(2) 确定控制区之间信息流动的访问控制策略。

① 从信任区到非军事区　源 IP 地址＝193.1.1.0/24　目的 IP 地址＝193.1.2.5/32　HTTP 服务;

② 从信任区到非军事区　源 IP 地址＝193.1.1.0/24　目的 IP 地址＝193.1.2.6/32　SMTP＋POP3 服务;

③ 从信任区到非信任区　源 IP 地址＝193.1.1.0/24　目的 IP 地址＝0.0.0.0　HTTP＋FTP GET 服务;

④ 从非军事区到非信任区　源 IP 地址＝193.1.2.6/32　目的 IP 地址＝0.0.0.0　SMTP 服务;

⑤ 从非信任区到非军事区　源 IP 地址＝0.0.0.0　目的 IP 地址＝193.1.2.5/32　HTTP GET 服务;

⑥ 从非信任区到非军事区　源 IP 地址＝0.0.0.0　目的 IP 地址＝193.1.2.6/32　SMTP 服务。

每一条访问控制策略给出三部分信息:一是信息流动方向,如策略 1 给出的从信任区到非军事区,二是允许启动信息交换过程的源终端地址范围和被动响应信息交换过程的目的终端地址范围,如策略 1 中允许启动信息交换过程的源终端是子网 193.1.1.0/24 内的任何终端,而允许被动响应信息交换过程的目的终端只能是 Web 服务器。三是以服务方式定义了整个信息交换过程。有状态分组过滤器如何实施上述访问控制策略呢?下

面以策略 1 为例，讨论一下防火墙实施信息交换控制的过程。

策略 1 表明允许由属于信任区的终端发起对非军事区内的 Web 服务器的访问，源 IP 地址范围表明信任区内有权发起对非军事区内的 Web 服务器访问的终端范围(193.1.1.0/24 指IP 地址为 193.1.1.0～193.1.1.255 的终端，0.0.0.0. 则指区内所有终端)，目的 IP 地址表明允许访问的非军事区内的 Web 服务器范围(193.1.2.5/32 指 IP 地址为 193.1.2.5 的服务器，0.0.0.0. 则指区内所有终端)。在讨论防火墙实现策略 1 的机制前，先给出由属于信任区的终端发起的访问非军事区内的 Web 服务器的过程中所涉及的信息交换过程，如图 7.6 所示。

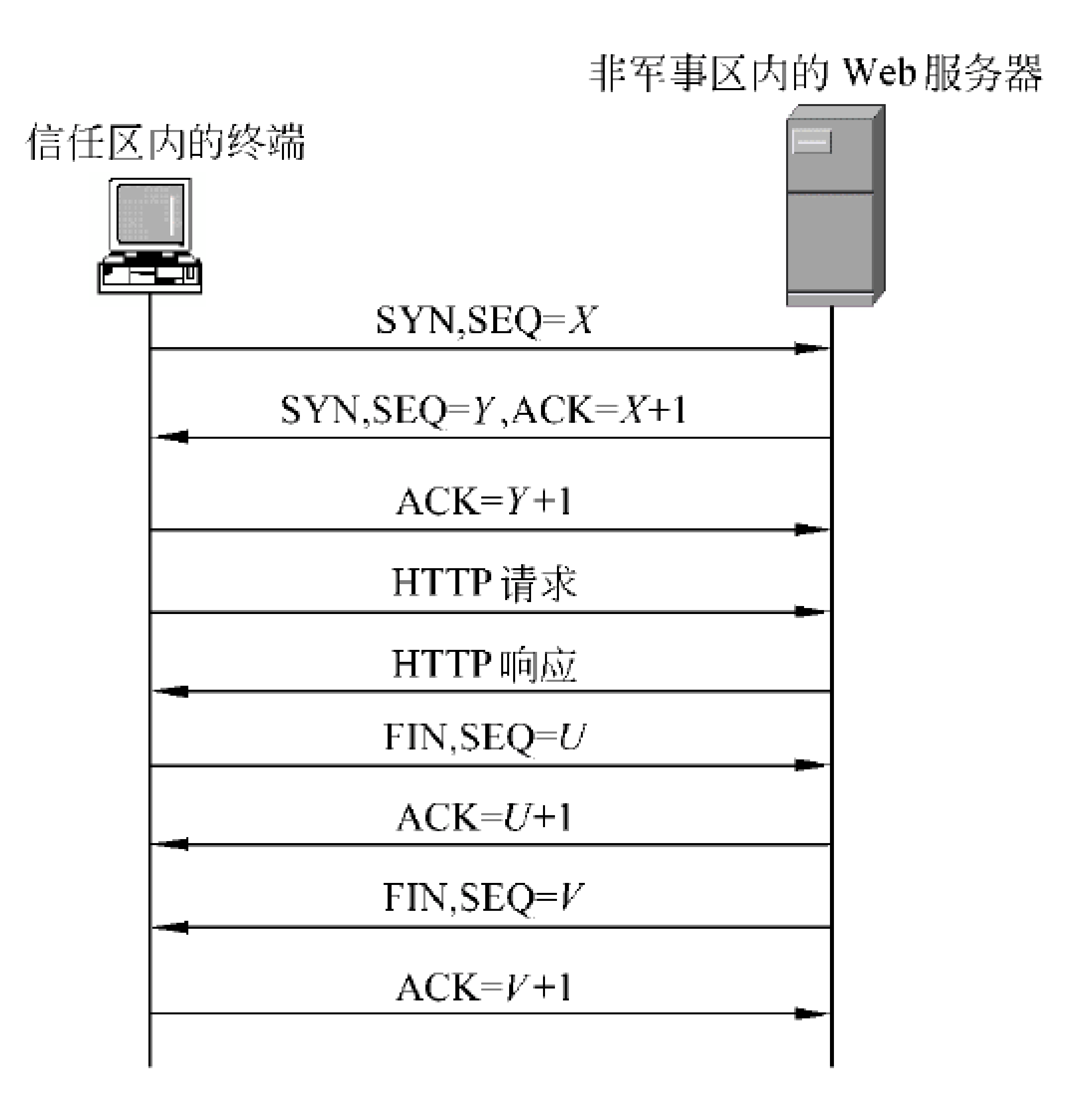


图 7.6　HTTP 服务信息交换过程

正确的信息交换过程是首先由属于信任区内的终端发起和非军事区内的 Web 服务器之间的 TCP 连接建立过程。建立 TCP 连接过程中，首先是由属于信任区内的终端发出的源 IP 地址＝193.1.1.0/24，目的 IP 地址＝193.1.2.5，目的端口号＝80，且 TCP 首部中 SYN＝1、ACK＝0 的建立 TCP 连接请求报文，其次是来自非军事区内的 Web 服务器的源 IP 地址＝193.1.2.5，目的 IP 地址＝193.1.1.0/24，源端口号＝80，且 TCP 首部中 SYN＝1、ACK＝1 的同意建立 TCP 连接的响应报文，最后是由属于信任区的终端发送的确认报文。了解了建立 TCP 连接的信息交换过程后，可以讨论一下防火墙控制上述信息交换过程的机制。防火墙为每一个 TCP 连接在连接表中建立一项，并且记录下 TCP 连接的状态，TCP 连接提供服务的对象。

当防火墙从端口 1 接收到 IP 分组(确定来自信任区)，它首先根据 IP 分组首部字段值(源 IP 地址和目的 IP 地址)，TCP 报文首部字段值(源端口和目的端口号)去检索 TCP 连接表，确定 TCP 连接表中是否存在和上述字段值匹配的连接项，如果没有，就去检索访问控制策略表，看访问控制策略表中是否存在允许建立该 TCP 连接的访问控制策略。在本例中，策略 1 允许建立由属于信任区内的终端发起的、和非军事区中的 Web 服务器之间的 TCP 连接，因此，在 TCP 连接表中检索不到对应连接项的情况下，根据策略 1，防火

墙端口1接收到的IP分组中，只有符合源IP地址＝193.1.1.0/24，目的IP地址＝193.1.2.5，目的端口号＝80，TCP报文首部中SYN＝1、ACK＝0的条件且转发端口为端口2的IP分组，才是允许继续传输的IP分组，同时在TCP连接表中建立一项，如表7.1所示。

表7.1　防火墙TCP连接表

源　终　端	目的终端	源端口号	目的端口号	状　　态	服务对象
193.1.1.1	193.1.2.5	1307	80	等待响应	HTTP

可以说，在TCP连接表中建立对应连接项前，根据策略1和策略2，当且仅当由属于信任区内终端发出的、请求和非军事区内的Web服务器或E-mail服务器建立TCP连接的TCP请求报文才允许继续传输，其他所有企图和信任区内终端通信的IP分组一律予以拒绝。

当防火墙从端口2(确定来自非军事区)接收到源IP地址＝193.1.2.5，目的IP地址＝193.1.1.1，源端口号＝80，目的端口号＝1307的TCP报文，根据报文中的多个特征字段值(如源和目的IP地址、源和目的端口号)去匹配TCP连接表，匹配到的对应项指出：该TCP连接是由IP地址＝192.1.1.1终端发起的，而且该TCP连接的后续报文应该是从IP地址为193.1.2.5的服务器发出的同意建立TCP连接的响应报文。防火墙检查该TCP报文首部中的SYN和ACK标志位是否为1，若为1，表明是响应报文，允许继续传输；否则，予以拒绝。在检测到响应报文后，TCP连接转为等待确认，这种状态下，当且仅当IP地址＝192.1.1.1的终端发出的TCP连接确认报文，才能继续传输，其他类型TCP报文都予以拒绝。在防火墙通过端口1接收到IP地址＝193.1.1.1的终端发出的确认报文后，TCP连接状态转变为建立。在这种情况下，防火墙从端口1接收到的TCP报文只有符合下述条件才允许继续传输：

① 和该TCP连接匹配；

② 是HTTP请求报文；

③ 发送序号在合理范围内。

同样，防火墙从端口2接收到的TCP报文也只有符合下述条件才能继续传输：

① 和该TCP连接匹配；

② 是HTTP响应报文；

③ 确认序号和另一方向发送的TCP报文的发送序号有合理关系。

从上述分析可以看出，在如此严密的控制下，攻击者要伪造能够欺骗防火墙的IP分组是何等困难，因此，只有提供有状态分组过滤器功能的防火墙才是真正意义上的防火墙，而无状态分组过滤器功能通常由路由器完成。

为了更好理解有状态分组过滤器的工作过程，用下面一个例子来进一步说明有状态分组过滤器控制区之间信息流动的过程。

【例7.1】 ①为什么策略2的服务是SMTP＋POP3，而策略4、策略6只是SMTP服务？②为什么要用策略4、策略6定义从非军事区到非信任区，从非信任区到非军事区的

SMTP 服务，而只需用策略 2 给出从信任区到非军事区的 SMTP＋POP3 服务。

【解析】 ① 对属于信任区内的终端而言，非军事区中的 E-mail 服务器是本地的邮件服务器，需要完成发送邮件和接收邮件的功能，而 SMTP 是用户向 E-mail 服务器发送邮件时使用的协议，POP3 是用户通过 E-mail 服务器接收邮件时使用的协议，因此，对属于信任区内的终端而言，非军事区内的邮件服务器必须提供 SMTP＋POP3 服务。而邮件服务器之间只需要相互发送邮件，因此，只需要用到 SMTP。

② 刚从无状态分组过滤器转到有状态分组过滤器的读者，很容易把策略 2 定义的从信任区到非军事区的 SMTP＋POP3 服务，看作是防火墙端口 1 允许来自信任区的、和通过 SMTP 或 POP3 访问非军事区的 E-mail 服务器相关的 IP 分组继续传输；否则，予以丢弃的过滤规则。为了达成双向传输，必须在防火墙端口 2 定义从非军事区的 E-mail 服务器到信任区内终端的 SMTP＋POP3 服务。其实把策略 2 定义的服务看作是分组过滤规则是完全抹杀了有状态分组过滤器通过服务来定义整个访问过程的能力。策略 2 实际允许在信任区和非军事区之间产生两个访问过程，如图 7.7 所示。这两个访问过程包含了在信任区和非军事区之间相互通信的 IP 分组，但防火墙只允许按照图 7.7 所示的访问过程进行交换的 IP 分组经过防火墙，否则予以丢弃。有状态分组过滤器的本质在于防火墙

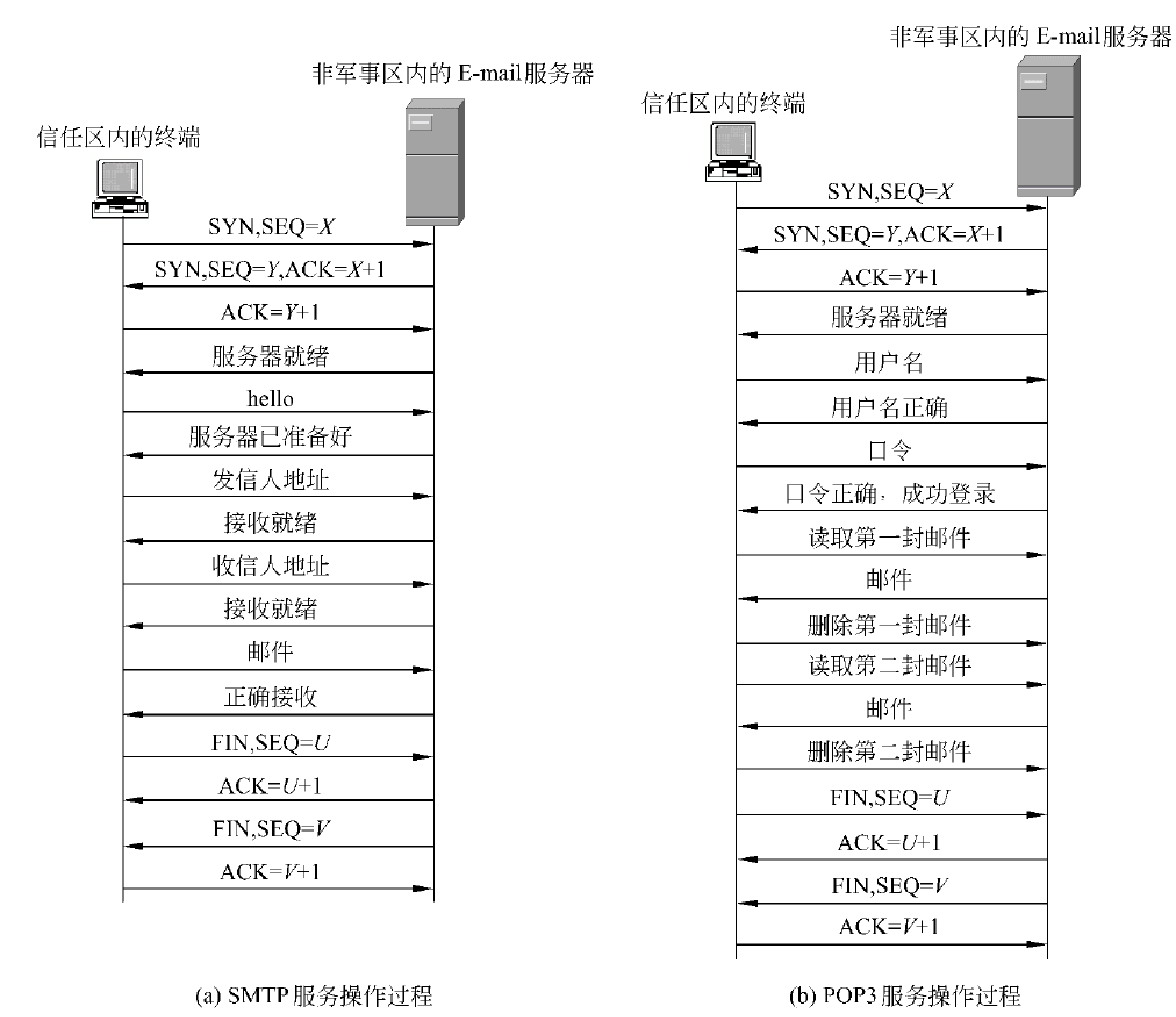


图 7.7 SMTP＋POP3 服务操作过程

记录下访问过程中每一个阶段的状态,以此决定那些 IP 分组是完成下一阶段操作所需要的,只有用于完成下一阶段操作的 IP 分组才能通过防火墙。如图 7.7(a)中,在第一个阶段开始时,只允许来自信任区的建立 TCP 连接的请求报文通过防火墙端口 1 进入防火墙,并通过防火墙端口 2 进入非军事区,随后,除了来自非军事区内的 E-mail 服务器的同意建立 TCP 连接的响应报文可以通过防火墙,其他 IP 分组一律予以拒绝。

至于为什么在非军事区和非信任区之间定义双向 SMTP 服务,是因为非军事区中的 E-mail 服务器可能发起向非信任区中 E-mail 服务器发送邮件的操作,同样,非信任区中的 E-mail 服务器也可能发起向非军事区中的 E-mail 服务器发送邮件的操作。

2. 有状态分组过滤器应用实例

图 7.8 是一个典型的校园网拓扑结构,内部网络被分为四个 VLAN,分别是 VLAN 1～VLAN 4,其中 VLAN 1 由管理终端组成,可以访问网络中一切资源,VLAN 2 由教师终端组成,允许向 FTP 服务器上传课件等信息,但只能访问 Web 服务器中的内容,VLAN 3 由学生终端组成,只能访问 FTP 和 Web 服务器中的内容。VLAN 4 由服务器组成,只能被动接受访问。这种配置下,图 7.5 中的信任区被分为四个不同的区,分别对应四个不同的 VLAN,因此称为管理员区、教师区、学生区和服务器区。四个 VLAN 分别分配子网地址 200.1.1.0/24、200.1.2.0/24、200.1.3.0/24 和 200.1.4.0/24。这样,防火墙端口 1 必须定义成四个不同的接口,分别连接四个不同的 VLAN,同时需要为四个不同的接口分配和所连接的 VLAN 子网地址一致的接口地址,如 200.1.1.254、200.1.2.254、200.1.3.254 和200.1.4.254。管理员区包含防火墙连接 VLAN 1 的接口,教师区包含防火墙连接 VLAN 2 的接口,学生区包含防火墙连接 VLAN 3 的接口,服务器区包含防火墙连接 VLAN 4 的接口。为了控制区之间的信息流动,需要在防火墙中定义如下访问控制策略:

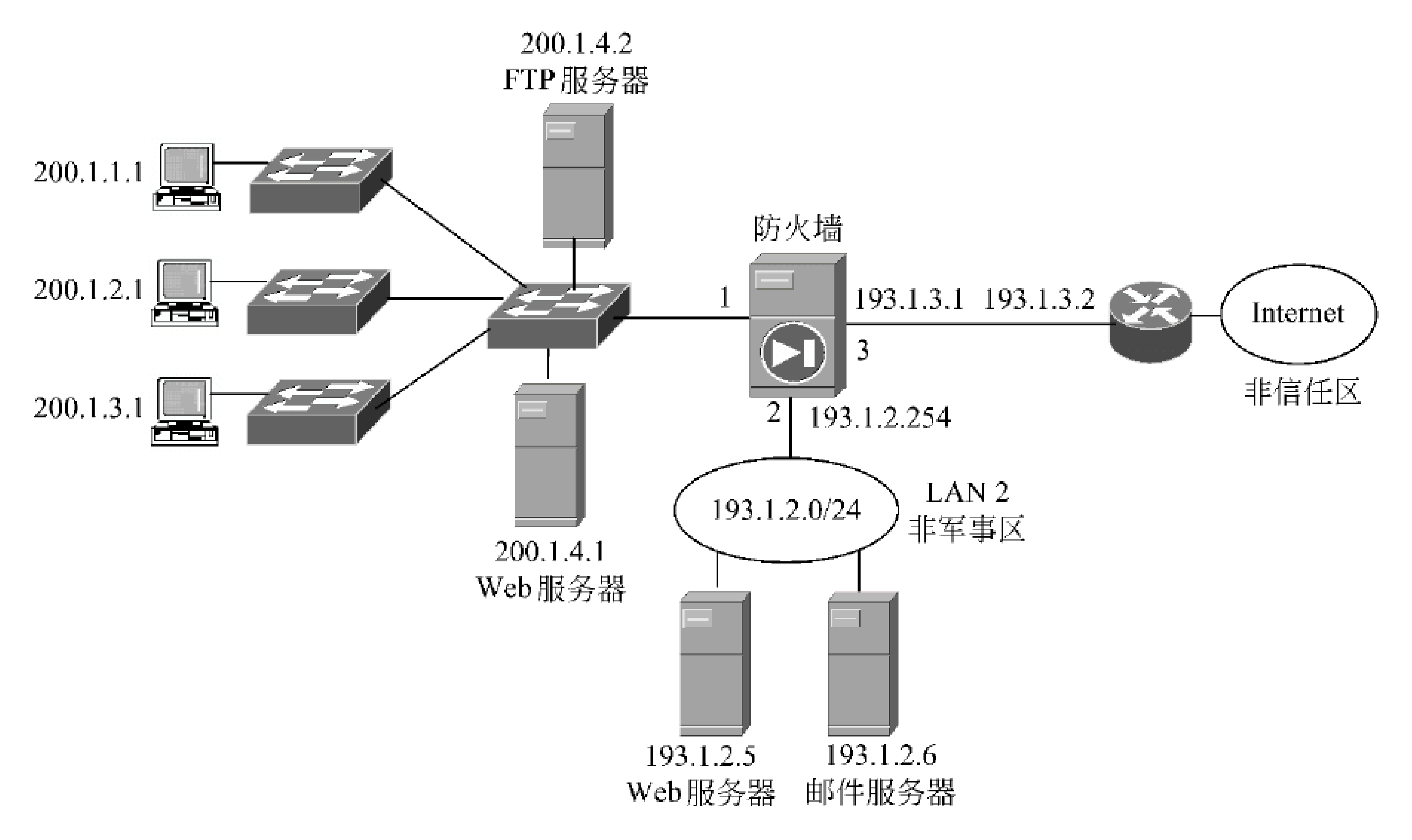


图 7.8 网络拓扑结构

(1) 从管理员区到非军事区　源 IP 地址＝200.1.1.0/24　目的 IP 地址＝193.1.2.5/32 HTTP＋Telnet 服务；

(2) 从管理员区到非军事区　源 IP 地址＝200.1.1.0/24　目的 IP 地址＝193.1.2.6/32 SMTP＋POP3＋Telnet 服务；

(3) 从管理员区到服务器区　源 IP 地址＝200.1.1.0/24　目的 IP 地址＝200.1.4.1/32 HTTP＋Telnet 服务；

(4) 从管理员区到服务器区　源 IP 地址＝200.1.1.0/24　目的 IP 地址＝200.1.4.2/32 FTP＋Telnet 服务；

(5) 从管理员区到教师区　源 IP 地址＝200.1.1.0/24　目的 IP 地址＝200.1.2.0/24 Telnet 服务；

(6) 管理员区到学生区　源 IP 地址＝200.1.1.0/24　目的 IP 地址＝200.1.3.0/24 Telnet 服务；

(7) 从管理员区到非信任区　源 IP 地址＝200.1.1.0/24　目的 IP 地址＝0.0.0.0 HTTP＋FTP GET 服务；

(8) 从教师区到非军事区　源 IP 地址＝200.1.2.0/24　目的 IP 地址＝193.1.2.5/32 HTTP GET 服务；

(9) 从教师区到非军事区　源 IP 地址＝200.1.2.0/24　目的 IP 地址＝193.1.2.6/32 SMTP＋POP3 服务；

(10) 从教师区到服务器区　源 IP 地址＝200.1.2.0/24　目的 IP 地址＝200.1.4.1/32 HTTP GET 服务；

(11) 从教师区到服务器区　源 IP 地址＝200.1.2.0/24　目的 IP 地址＝200.1.4.2/32 FTP 服务；

(12) 从教师区到非信任区　源 IP 地址＝200.1.2.0/24　目的 IP 地址＝0.0.0.0　HTTP＋FTP GET 服务；

(13) 从学生区到非军事区　源 IP 地址＝200.1.3.0/24　目的 IP 地址＝193.1.2.5/32 HTTP GET 服务；

(14) 从学生区到非军事区　源 IP 地址＝200.1.3.0/24　目的 IP 地址＝193.1.2.6/32 SMTP＋POP3 服务；

(15) 从学生区到服务器区　源 IP 地址＝200.1.3.0/24　目的 IP 地址＝200.1.4.1/32 HTTP GET 服务；

(16) 从学生区到服务器区　源 IP 地址＝200.1.3.0/24　目的 IP 地址＝200.1.4.2/32 FTP GET 服务；

(17) 从学生区到非信任区　源 IP 地址＝200.1.2.0/24　目的 IP 地址＝0.0.0.0 HTTP＋FTP GET 服务；

(18) 从非军事区到非信任区　源 IP 地址＝193.1.2.6/32　目的 IP 地址＝0.0.0.0 SMTP 服务；

(19) 从非信任区到非军事区　源 IP 地址＝0.0.0.0　目的 IP 地址＝193.1.2.5/32 HTTP GET 服务；

(20) 从非信任区到非军事区　源 IP 地址＝0.0.0.0　目的 IP 地址＝193.1.2.6/32 SMTP 服务。

内部网络中，除了来自非信任区的攻击外，还有来自内部网络中感染了病毒的终端发起的攻击，而且，来自内部网络中终端的拒绝服务攻击是导致内部网络发生拥塞的主要原因，因此，对内部网络分区，并通过访问控制策略有效控制内部网络中各个 VLAN 之间的信息交换过程是解决内部网络因为遭受内部终端发起的拒绝服务攻击而导致的拥塞的有效办法。当然，这种通过分区和设置访问控制策略的机制并不能解决所有网络攻击，如果感染病毒的学生终端通过发送大量的 ICMP 报文来阻塞连接 FTP 服务器的链路，由于学生区和服务器区之间的访问控制策略不允许 ICMP 报文在这两区之间传输，这种攻击无法得逞。但如果感染病毒的学生终端通过 SYN 泛洪攻击来终止 FTP 服务器的正常服务功能，控制学生区和服务器区之间信息流动的访问控制策略是无法阻止这种攻击的。

3. 有状态分组过滤器其他防攻击机制

1) 防 SYN 泛洪攻击

拒绝服务(DoS)攻击是利用访问权限允许的访问过程不正常地发送请求或其他信息，导致服务器不能正常提供服务或网络结点发生拥塞的一种攻击手段，由于这种攻击手段并不违背访问控制策略，因此，无法通过控制区之间的信息流动有效抑制这种攻击，如图 7.8 中非信任区中的网络终端通过 SYS 泛洪来终止非军事区中的 Web 服务器的正常服务功能的拒绝服务攻击，是无法通过控制区之间的信息流动的访问控制策略解决的，甚至防火墙中的 TCP 连接表也有可能因溢出而无法正常工作。因此，防火墙必须在有状态报文过滤器的功能上，增加防拒绝服务攻击的能力。

下面通过防火墙防 SYN 泛洪攻击的机制来讨论一下防火墙防拒绝服务(DoS)攻击的工作原理。假定图 7.8 所示网络的非信任区中的用户用 SYN 泛洪攻击手段攻击非军事区内的 Web 服务器，如图 7.9 所示。

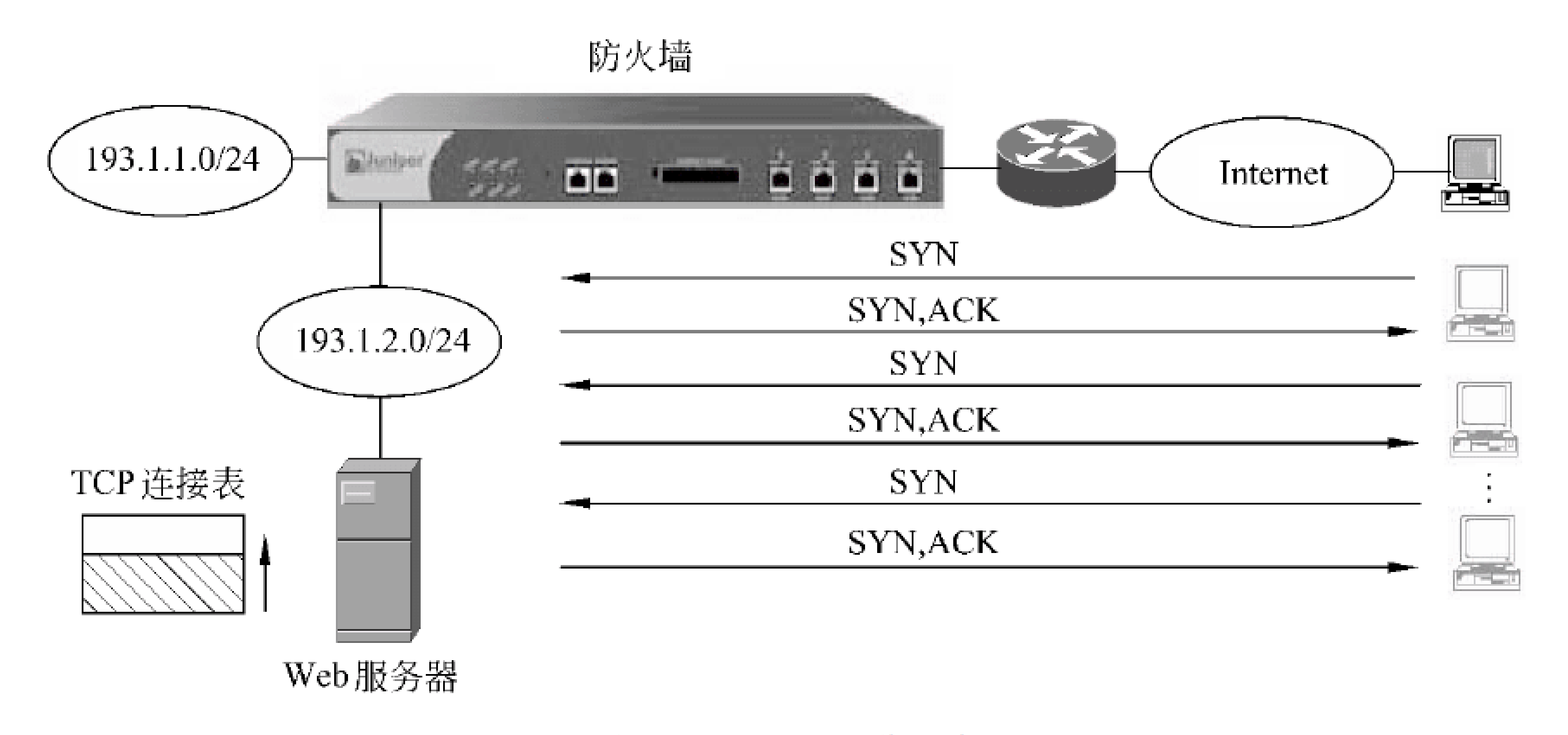


图 7.9　SYN 泛洪攻击

TCP 连接建立过程需要三次握手操作，如图 7.6 和图 7.7 所示的 TCP 连接建立过程。客户端发送 SYN＝1 的建立 TCP 连接请求报文，服务器回送 SYN＝1、ACK＝1 的同意建立 TCP 连接的响应报文，服务器在发送响应报文后，等待客户端的确认报文，在这

等待阶段,服务器端已经在 TCP 连接表中建立对应项。如果直到等待时间(60 秒～2 分种)溢出,服务器端仍未接收到来自客户端的确认报文,认为无法建立 TCP 连接,终止连接建立过程,并从 TCP 连接表中删除已经建立的对应项。这就意味着只要非信任区中某个用户持续以本不存在的终端地址向服务器发送 SYN=1 的建立 TCP 连接请求报文,服务器端等待客户端确认报文的未完全建立的 TCP 连接数量将急剧增加,最终导致 TCP 连接表溢出,使得正常访问服务器的客户因为无法和服务器建立 TCP 连接而宣告失败。

为了防 SYN 泛洪攻击,在防火墙连接非信任区的端口启动防 SYN 泛洪攻击机制,它的操作过程如下:首先设定每秒允许由非信任区内终端发送给非军事区内 Web 服务器的建立 TCP 连接请求报文(SYN=1,ACK=0 的 TCP 报文)的数量,这个数量应该大于峰值情况下 Web 服务器每秒建立的 TCP 连接数。假定设定每秒允许经过防火墙送往非军事区的建立 TCP 连接请求报文数为 500,那么,在允许的到达速率内,非信任区发送给 Web 服务器的建立 TCP 连接请求报文经过防火墙直接转发给 Web 服务器。一旦,来自非信任区的建立 TCP 连接请求报文的到达速率超过 500 个/秒,防火墙将超过设定到达速率的建立 TCP 连接请求报文(1 秒内到达的第 501 个及以后的建立 TCP 连接请求报文)拦截,并由防火墙向客户端发送同意建立 TCP 连接的响应报文(SYN=1、ACK=1),只有在接收到来自客户端的确认报文后,再真正和 Web 服务器建立 TCP 连接。当然,防火墙作为代理需要对来自客户端的 TCP 报文的确认序号和来自服务器端的 TCP 报文的发送序号进行调整,整个过程如图 7.10 所示。

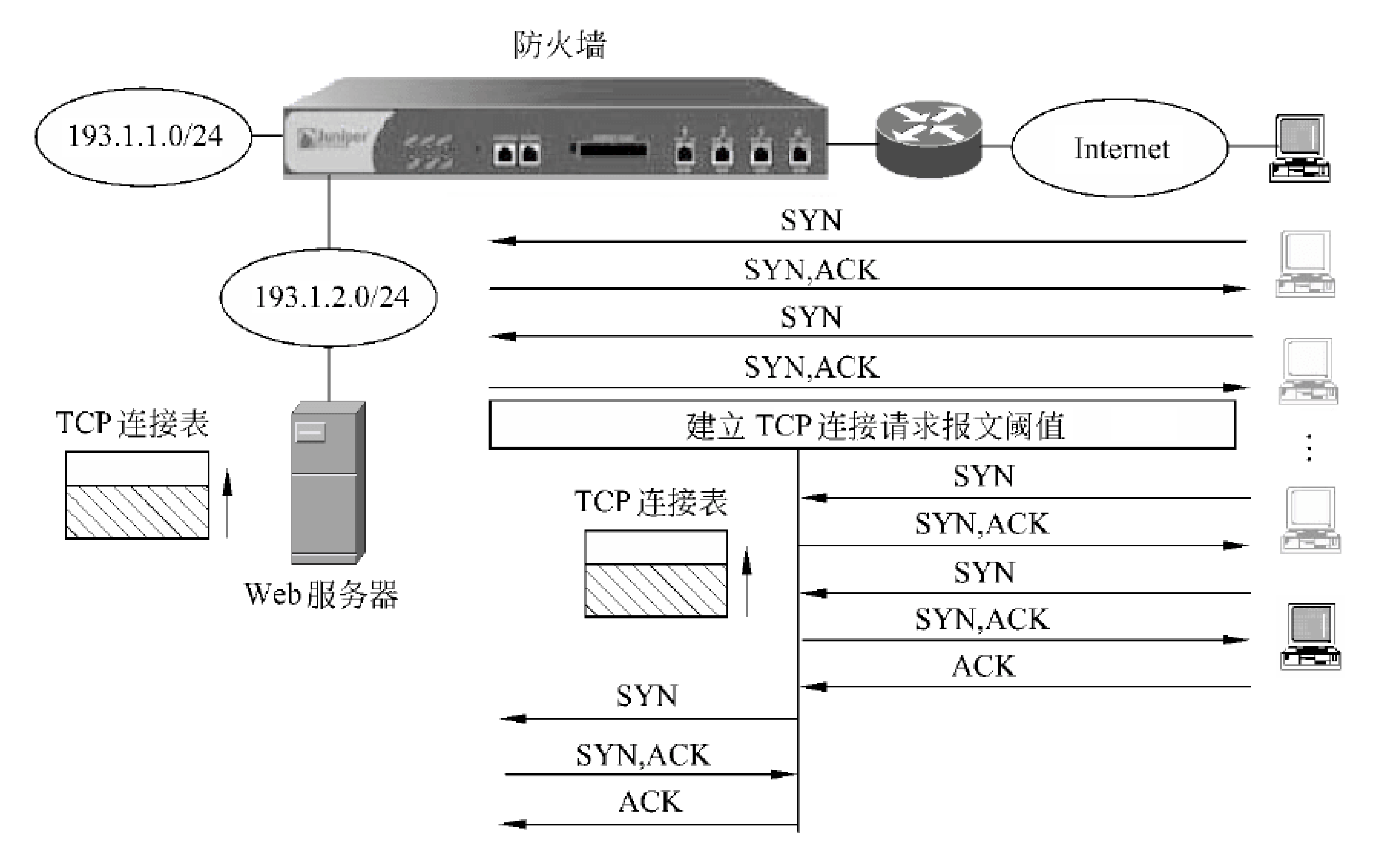


图 7.10 防火墙防 SYN 泛洪攻击过程

从图 7.10 中看出,防火墙防 SYN 泛洪攻击的机制是把原本由服务器承担的负荷转移到自己身上,但自己的 TCP 连接表也存在溢出问题,因此,防火墙也设定允许接收 SYN=1 的建立 TCP 连接请求报文的最高速率,超过该到达速率的建立 TCP 连接请求

报文将直接被防火墙丢弃，同时向网络管理平台报警。

另一种可以使防火墙免于在 TCP 连接表中记录大量未完成的 TCP 连接的技术是 Cookie 技术。采用 Cookie 技术，防火墙只对完成三次握手过程、成功建立的 TCP 连接进行策略控制，并在通过策略控制的情况下，在 TCP 连接表中创建对应项，并以代理方式与 Web 服务器建立 TCP 连接，如图 7.11 所示。在图 7.11 中，一旦到达的 SYN＝1 的建立 TCP 连接请求报文已经超过设定的到达速率，防火墙拦截下该请求报文，并由防火墙发送 SYN＝1、ACK＝1 的响应报文，但响应报文中给出的初始发送序号（见图 7.11 中的 Z_1、Z_2）＝MD5（请求报文源 IP 地址，目的 IP 地址，源端口号，目的端口号，初始发送序号）。防火墙发送响应报文后，并不在 TCP 连接表中记录任何信息，那么，当防火墙接收到来自客户端的确认报文时，如何在 TCP 连接表中创建对应的连接项呢？防火墙重新计算 MD5（确认报文的源 IP 地址，目的 IP 地址，源端口号，目的端口号，发送序号－1），并把计算结果和减 1 后的确认序号比较，如果相等，意味着该确认报文和通过 Cookie 技术生成的响应报文是对应的，并因此在 TCP 连接表中创建连接项，并继而和 Web 服务器建立 TCP 连接。当然，由于防火墙的代理作用，客户端的初始确认序号和服务器端的初始发送序号并不一致，需要防火墙进行修正。

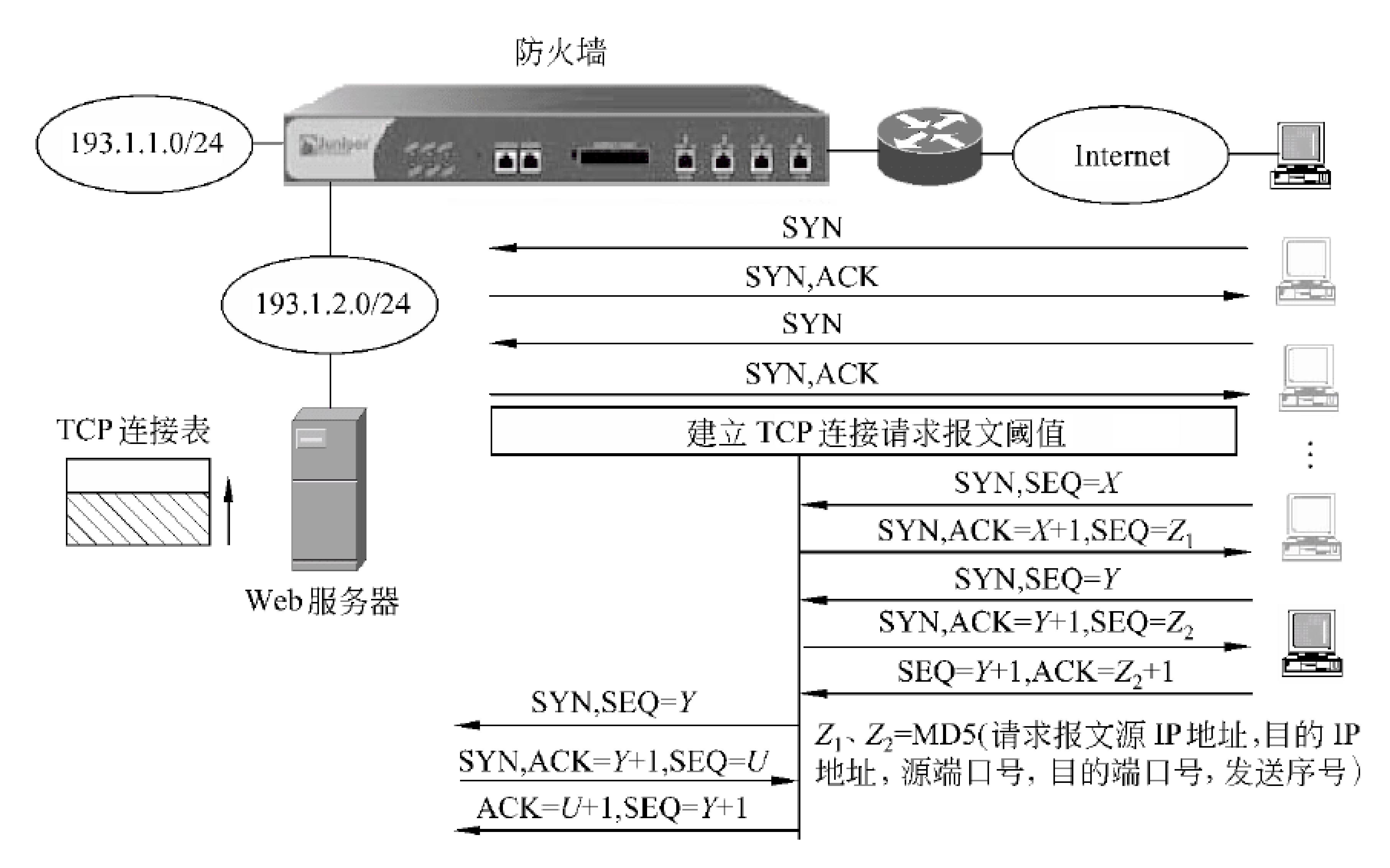


图 7.11　用 Cookie 技术解决 TCP 连接表溢出问题

2）防侦察机制

黑客发起攻击前，首先需要确定目标，了解目标信息，掌握目标的弱点，然后有针对性地实施对目标的攻击。确定目标是在网络中发现一个可以攻击的对象，这个对象必须连接在网络上，有些端口是打开的。黑客通过 IP 地址扫描来发现某个连接在网络的对象，通过端口扫描来发现该对象某些打开的端口，通常情况下，黑客通过发送目的 IP 地址递增的 ICMP ECHO 请求报文来发现某个连接在网络上的对象，因为，一旦黑客接收到某个 ICMP ECHO 响应报文，意味着黑客可以到达发送该 ICMP ECHO 响应报文的终端，

可以把该终端作为实施攻击的对象。然后，黑客通过发送目的端口号递增的 SYN=1 的建立 TCP 连接请求报文来发现该对象某些打开的端口，因为，一旦接收到 SYN=1 和 ACK=1 的建立 TCP 连接响应报文，表明该响应报文的源端口号是打开的。为了掌握该对象的弱点，首先需要了解该对象使用的操作系统及版本，因为，不同操作系统，和同一操作系统的不同版本，其漏洞是不同的，只要掌握了对象使用的操作系统的漏洞，实施攻击就是一件轻而易举的事情。在 TCP 连接建立、维持和释放过程中，不同操作系统对异常情况的处理方式是不同的，黑客通过比较对象所使用的操作系统对某些特定异常情况的处理来确定对象所使用的操作系统类型及版本。

防火墙防 IP 地址扫描机制如图 7.12 所示，假定要防止来自非信任区的 IP 地址扫描侦察，在防火墙连接非信任区的端口启动防 IP 地址扫描机制，并设置时间间隔和阈值，如 5ms 和 10 个 ICMP ECHO 请求报文，端口在每一个时间段（这里为 5ms）检测具有相同源 IP 地址、不同目的 IP 地址的 ICMP ECHO 请求报文，允许前 10 个具有上述特征的 ICMP ECHO 请求报文通过端口继续转发，丢弃后续具有上述特征的 ICMP ECHO 请求报文，直到下一个时间段开始。这就保证对于特定的源终端，每一个时间段最多扫描 10 个不同的终端。

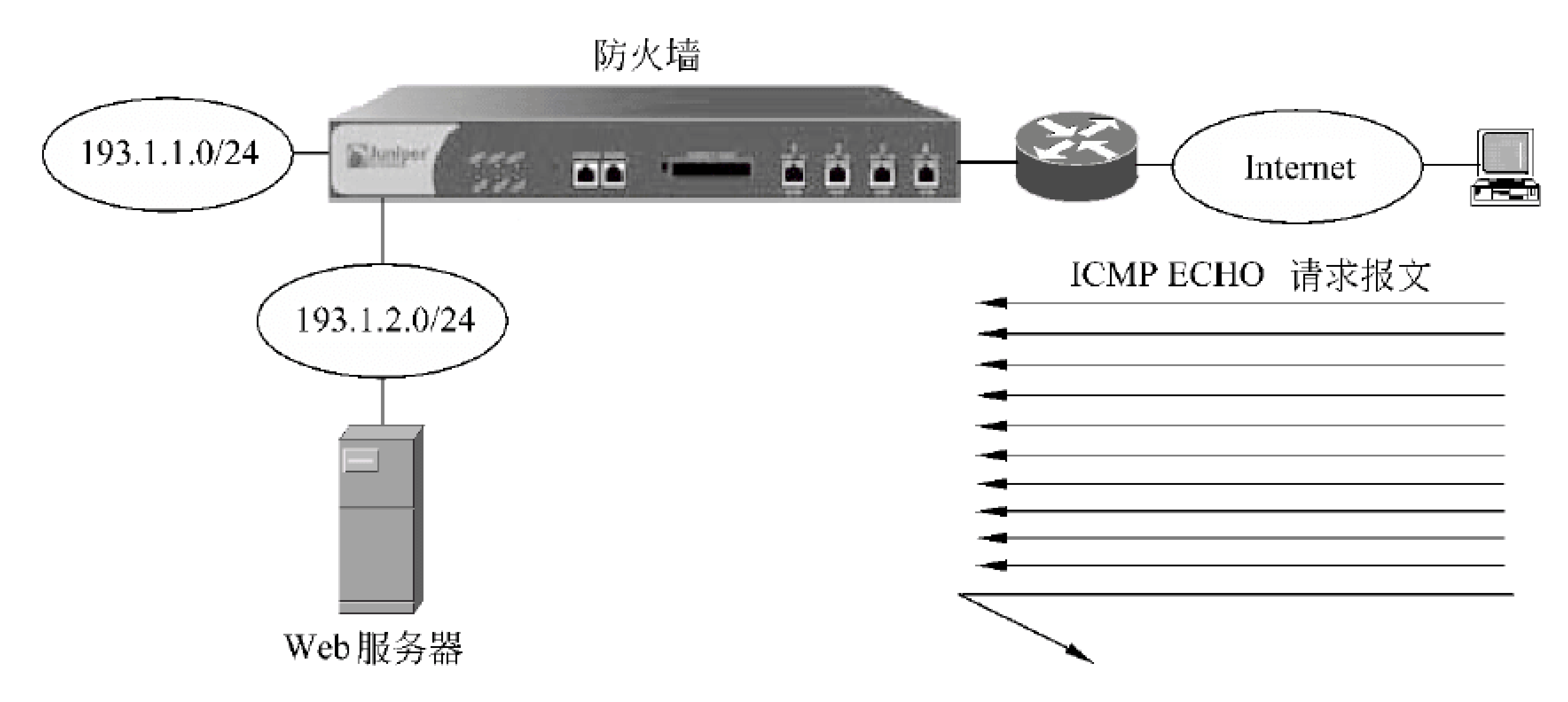


图 7.12 防火墙防 IP 地址扫描机制

防火墙防端口扫描机制和防 IP 地址扫描机制相似，在连接非信任区的端口启动防端口扫描机制后，也需要设置时间间隔和阈值，这两个参数决定了规定时间内允许通过端口转发的具有相同源和目的 IP 地址，不同目的端口号的 SYN=1 的建立 TCP 连接请求报文数。

由于控制区之间信息流动的访问控制策略可以设定每一个区内允许区间信息交换的 IP 地址范围和信息类型，因此，可以通过访问控制策略较好地解决防止一个区内的终端对另一个区实施 IP 地址扫描和端口扫描等侦察手段的问题。

TCP 连接建立、维持和释放过程中的异常情况是指 TCP 首部中出现控制位 FIN=1 和 ACK=0、SYN=1 等不允许同时出现的控制位置位情况，不同操作系统对这些异常情况的处理方式不同，有的操作系统忽略这些异常情况，有的操作系统一旦发现这样的异常情况就终止 TCP 连接并发送控制位 RST=1 的 TCP 报文。这样使得黑客终端可以通过发送控制位异常置位的 TCP 报文，和目的终端对这种异常 TCP 报文的响应来推断目的

终端使用的操作系统类型和版本。如果防火墙某个端口启动了防操作系统探测机制，防火墙对通过该端口接收到的所有 TCP 报文先检测是否存在控制位异常置位的情况，只有控制位置位符合 TCP 规范的 TCP 报文才允许继续转发，所有控制位异常置位的 TCP 报文都将丢弃，不再继续传输。由于这些控制位异常置位的 TCP 报文无法到达目的终端，黑客终端无法通过比较目的终端对这些控制位异常置位的 TCP 报文的响应方式来推断出目的终端所使用的操作系统类型及版本。

3）防源 IP 地址欺骗攻击

假定图 7.13 中整个内网划分为一个信任区，但这一信任区仍然由四个子网组成（VLAN 1～VLAN 4），对应的子网地址分别为 200.1.1.0/24、200.1.2.0/24、200.1.3.0/24 和200.1.4.0/24，防火墙端口 1 同样被定义为四个接口（1.1～1.4），分别连接四个 VLAN，但这四个接口同属于信任区。对不同 VLAN 中的终端分配不同的权限，如管理员终端对应的子网（VLAN 1，200.1.1.0/24）允许对非军事区内的 Web 服务器进行读写操作，而学生终端对应的子网（VLAN 3，200.1.3.0/24）只允许访问非军事区内的 Web 服务器，通过如下访问控制策略实现不同子网的权限分配。

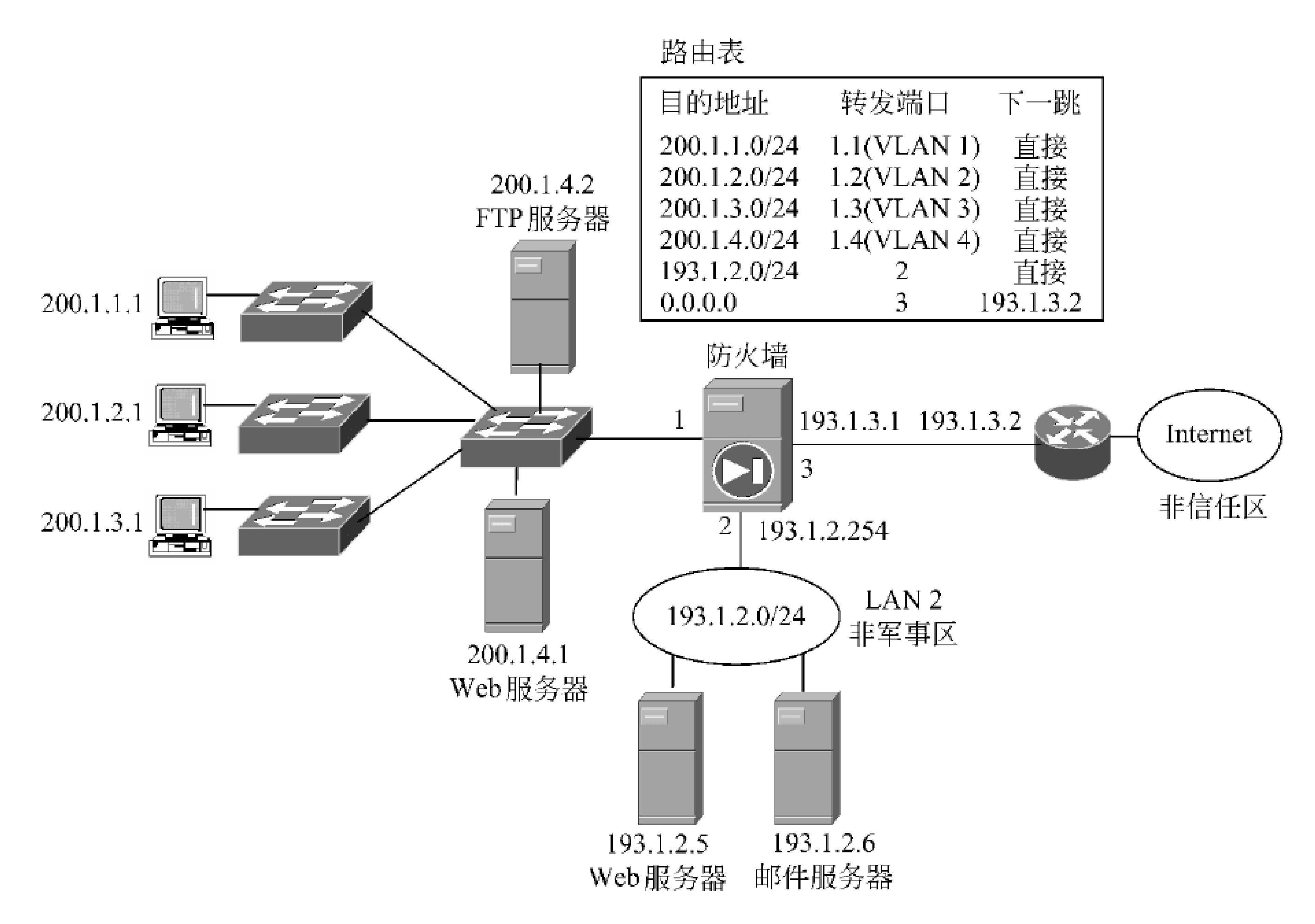


图 7.13　网络结构及路由表配置

（1）从信任区到非军事区 源 IP 地址＝200.1.1.0/24 目的 IP 地址＝193.1.2.5/32 HTTP＋Telnet 服务；

（2）从信任区到非军事区 源 IP 地址＝200.1.3.0/24 目的 IP 地址＝193.1.2.5/32 HTTP GET 服务。

问题是 IP 地址为 200.1.3.1 的学生终端通过将自己的 IP 地址伪造成 200.1.1.1，有可能将包含 HTTP PUT 命令的 HTTP 请求报文发送给非军事区中的 Web 服务器，从

而达到修改 Web 页面的目的，这是因为如果 IP 地址为 200.1.1.1 的管理员终端已经在防火墙中创建了和非军事区中的 Web 服务器进行 HTTP 服务的会话，学生终端伪造的源 IP 地址为 200.1.1.1 的包含 HTTP PUT 命令的 HTTP 请求报文有可能和该会话匹配，从而到达非军事区中的 Web 服务器。造成这一问题的根本原因是防火墙只检测输入该 IP 分组的接口所属的区，并不检测接口所连接的子网地址是否和该 IP 分组的源 IP 地址匹配。在上例中，由于输入该 IP 分组的接口 1.3(和 VLAN 3 对应)属于信任区，该 IP 分组的输入区确定为信任区，在该 IP 分组和会话表中某个会话匹配时，防火墙正常转发该 IP 分组。实际上，只要根据防火墙的路由表检索一下该 IP 分组源 IP 地址对应的输出接口，就会发现，根据源 IP 地址 200.1.1.1 检索路由表得到的输出接口是 1.1，而不是输入该 IP 分组的接口 1.3，这就表明源终端本应该连接在接口 1.1 连接的子网上，实际上却从接口 1.3 连接的子网上接收到该 IP 分组，这种情况表明该 IP 分组的实际传输路径和源 IP 地址指定终端至防火墙的传输路径不同，以此可以确定该 IP 分组的源 IP 地址是伪造的。防火墙如果在属于信任区的接口启动防源 IP 地址欺骗攻击，则在通过某个属于信任区的接口接收到 IP 分组后，即以该 IP 分组的源 IP 地址检索路由表，如果发现检索到的输出接口和接收该 IP 分组的接口不符，表明该 IP 分组的源 IP 地址是伪造的，丢弃该 IP 分组。

7.3 堡垒主机

堡垒主机是代理形式的应用层网关，代理形式表明堡垒主机对终端是不透明的，外网终端需要访问内部网络服务器时，首先和堡垒主机建立 TCP 连接，堡垒主机在通过对终端用户的身份认证后，再和内部网络服务器建立 TCP 连接。应用层网关表明堡垒主机对经过 TCP 连接传输的应用层报文进行检测，从语法、参数正确性，到资源地址和内容。

7.3.1 网络结构

1. 单穴堡垒主机结构

用单穴堡垒主机保护内部网络的网络结构如图 7.14 所示，单穴堡垒主机是指只有单个接口连接网络的堡垒主机，在图 7.14 所示的网络结构中，为了保证内部网络和 Internet 之间的通信必须经过堡垒主机，必须在无状态分组过滤器端口 1 的输入方向上设置只允许堡垒主机发送的信息才能正常传输到 Internet 的输入过滤器，在输出方向上设置只允许目的地为堡垒主机的信息才能进入内部网络的输出过滤器。

端口 1 输入方向过滤器：

源 IP 地址＝193.1.1.1 .and. 目的 IP 地址＝0.0.0.0　正常转发

源 IP 地址＝0.0.0.0 .and. 目的 IP 地址＝0.0.0.0　丢弃

端口 1 输出方向过滤器：

源 IP 地址＝0.0.0.0 .and. 目的 IP 地址＝193.1.1.1　正常转发

源 IP 地址＝0.0.0.0 .and. 目的 IP 地址＝0.0.0.0　丢弃

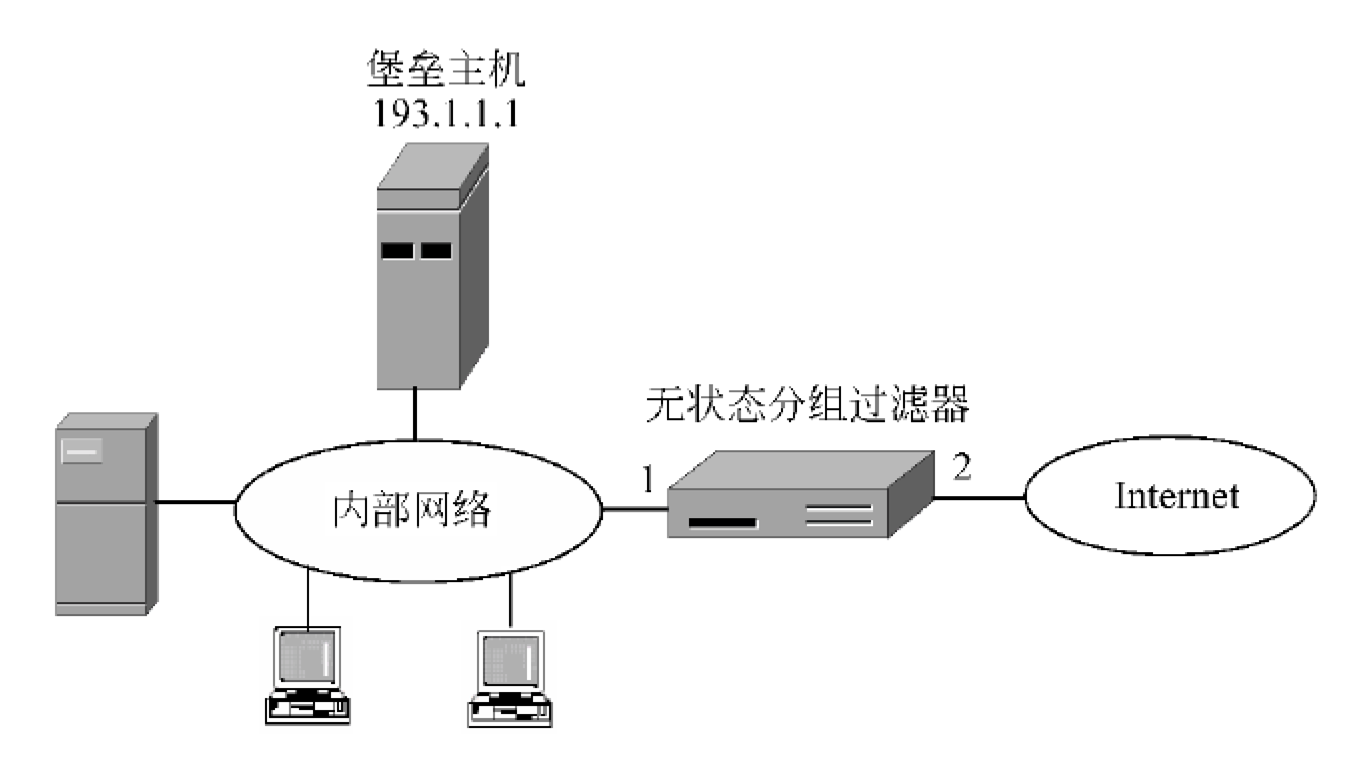


图 7.14　单穴堡垒主机结构

2. 双穴堡垒主机结构

图 7.14 所示的用单穴堡垒主机保护内部网络的网络结构存在无状态分组过滤器和内部网络中其他终端之间的传输通路，保证内部网络和 Internet 之间通信必须经过堡垒主机的关键是无状态分组过滤器端口 1 输入输出方向上设置的过滤器，一旦过滤器出现问题，内部网络中的终端和 Internet 之间可能出现直接通信的情况，这样，用堡垒主机保护内部网络资源的愿望可能落空。为了强迫内部网络和 Internet 之间的通信经过堡垒主机，可以采用双穴堡垒主机并采用图 7.15 所示的网络结构。双穴堡垒主机是指具有两个接口，允许同时和两个不同的网络连接的堡垒主机。对于图 7.15 所示的网络结构，即使无状态分组过滤器出现问题，也能保证内部网络和 Internet 之间的通信经过堡垒主机。

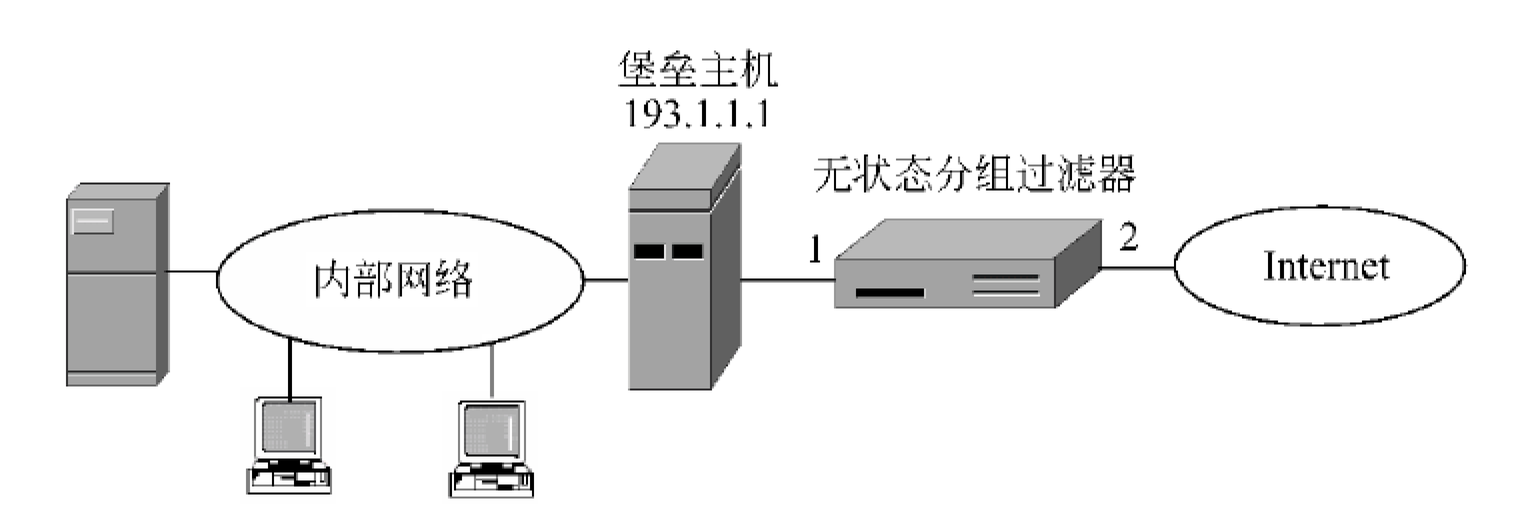


图 7.15　双穴堡垒主机结构

3. 双无状态分组过滤器结构

图 7.16 所示的网络结构，根据安全等级，将内部网络分成两部分：堡垒主机和内部

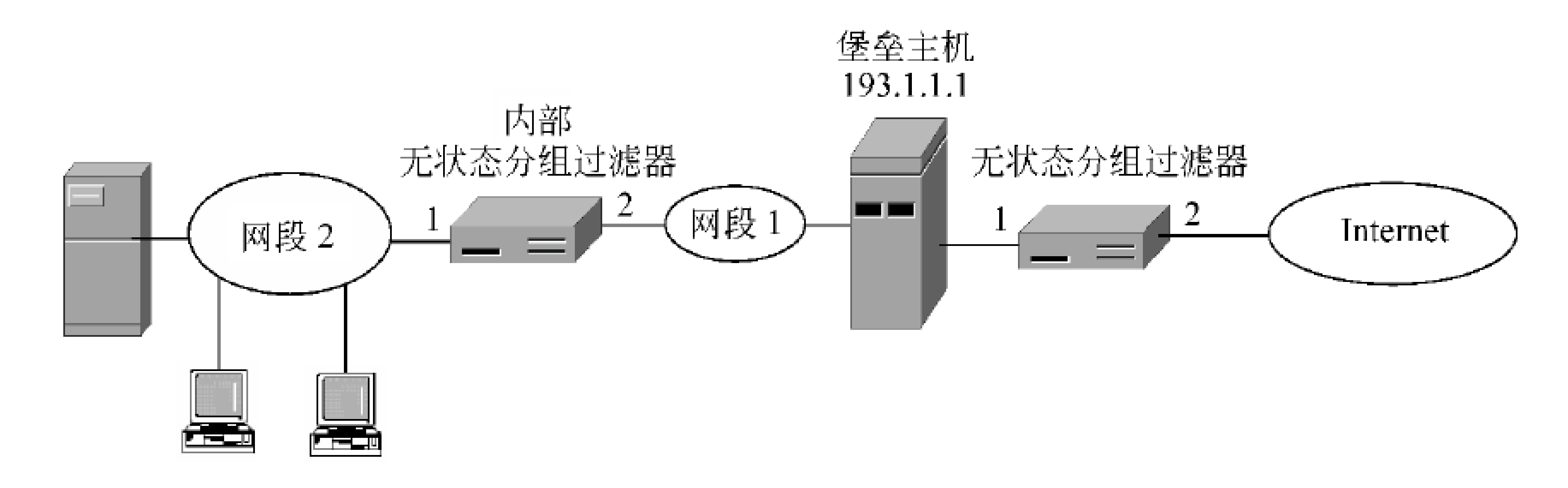


图 7.16　双无状态分组过滤器结构

无状态分组过滤器之间的网络段和内部无状态分组过滤器保护的网络段，这两个网络段有点类似于图 7.5 中的非军事区和信任区，这样，可以将不同安全等级的网络资源放在合适的网络段中。

7.3.2 堡垒主机工作机制

对于图 7.17 所示的网络结构，外网终端访问内部网络中 Web 服务器的过程如下：

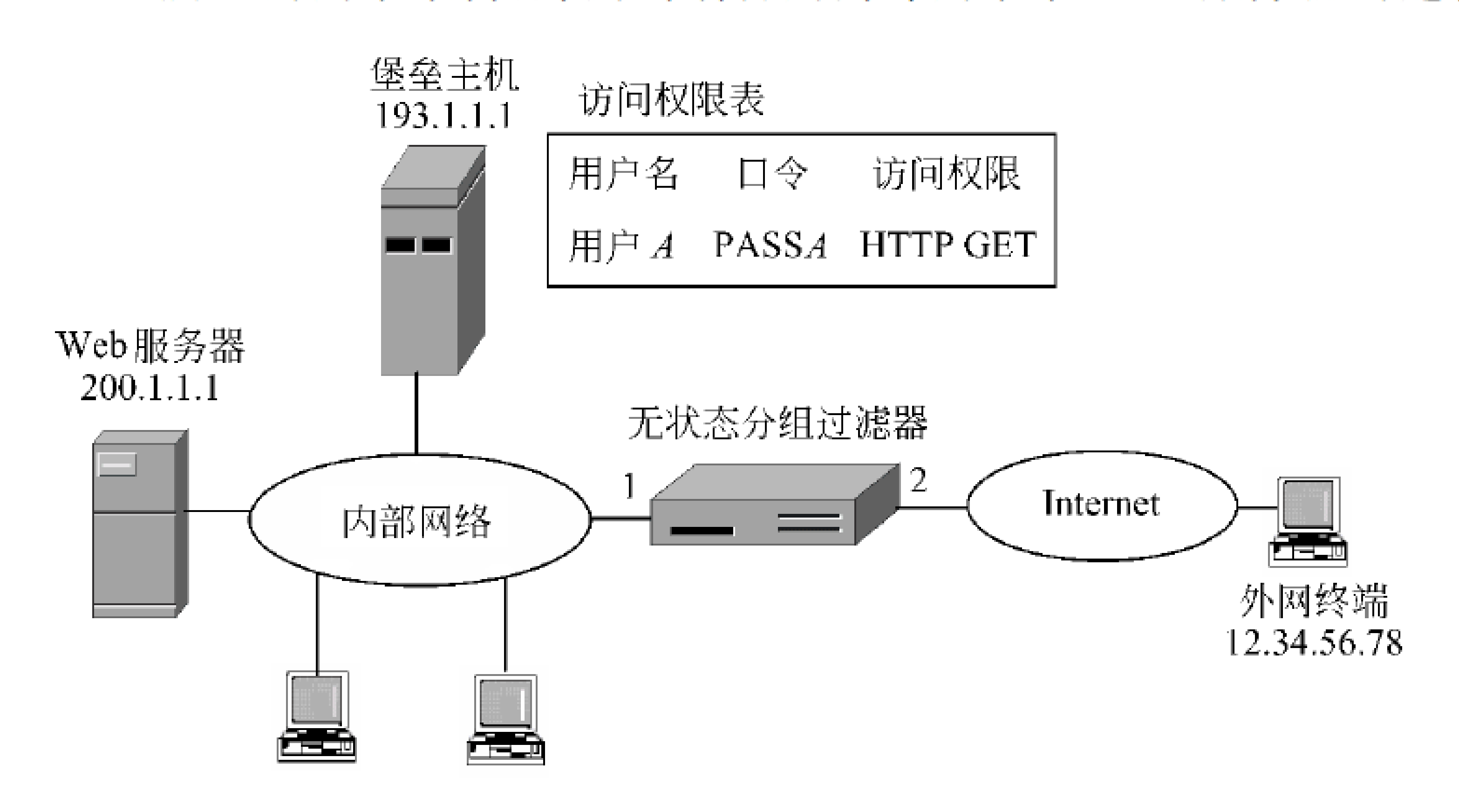


图 7.17 网络结构

(1) 在无状态分组过滤器端口 1 输入输出方向上设置如下过滤器：

端口 1 输入方向过滤器

源 IP 地址＝193.1.1.1 .and. 目的 IP 地址＝0.0.0.0 正常转发

源 IP 地址＝0.0.0.0 .and. 目的 IP 地址＝0.0.0.0 丢弃

端口 1 输出方向过滤器

源 IP 地址＝0.0.0.0 .and. 目的 IP 地址＝193.1.1.1 正常转发

源 IP 地址＝0.0.0.0 .and. 目的 IP 地址＝0.0.0.0 丢弃

以此保证外网终端必须通过堡垒主机才能访问内部网络资源。

(2) 外网终端必须先和堡垒主机建立 TCP 连接，在成功建立 TCP 连接后，通过向外网终端推送认证页面，对外网终端用户身份进行认证，如图 7.18 所示。假定外网终端用户的用户名为用户 A，口令为 PASSA，堡垒主机通过访问权限表获知允许用户 A 访问内部网络 Web 服务器，在外网终端提出访问内部网络 Web 服务器的请求后，和内部网络

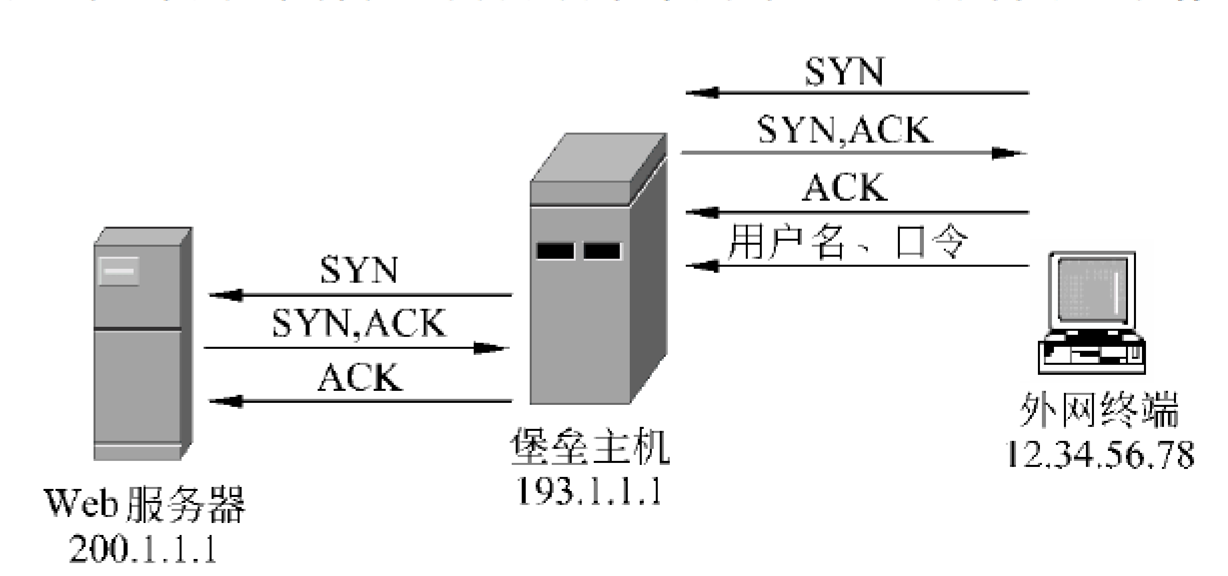


图 7.18 网络结构

Web 服务器建立 TCP 连接，并将这两个 TCP 连接绑定在一起，如表 7.2 所示，作为插口一部分的源和目的端口号在建立 TCP 连接时选定。

表 7.2　TCP 连接绑定表

终端和堡垒主机之间 TCP 连接		堡垒主机和 Web 服务器之间 TCP 连接		应用层服务
源　插　口	目 的 插 口	源　插　口	目 的 插 口	
12.34.56.78:1122	193.1.1.1:1180	193.1.1.1:2276	200.1.1.1:80	HTTP GET

(3) 外网终端先将发送给 Web 服务器的 HTTP 请求报文封装成以 12.34.56.78:1122 为源插口，以 193.1.1.1:1180 为目的插口的 TCP 报文，然后将该 TCP 报文发送给堡垒主机，堡垒主机首先根据 TCP 报文的源和目的插口在 TCP 连接绑定表中进行匹配操作，在匹配成功后，从 TCP 报文中分离出 HTTP 请求报文，首先检测 HTTP 请求报文的语法和参数的正确性，在确认正确无误后，根据 TCP 连接绑定表中给出的应用层服务检测 HTTP 请求报文中请求的服务(这里假定为 HTTP GET 服务)，在一致的情况下，由堡垒主机重新将 HTTP 请求报文封装成以 193.1.1.1:2276 为源插口，以 200.1.1.1:80 为目的插口的 TCP 报文，并将该 TCP 报文发送给 Web 服务器。

(4) Web 服务器完成 HTTP 请求报文所请求的服务，将 HTTP 响应报文封装成以 200.1.1.1:80 为源插口，以 193.1.1.1:2276 为目的插口的 TCP 报文，然后将该 TCP 报文发送给堡垒主机，堡垒主机完成 TCP 连接匹配和 HTTP 响应报文正确性检测后，重新将 HTTP 响应报文封装成以 193.1.1.1:1180 为源插口，以 12.34.56.78:1122 为目的插口的 TCP 报文，然后将该 TCP 报文发送给外网终端，完成外网终端和 Web 服务器之间的请求和响应过程。

7.3.3　堡垒主机功能特性

通过对堡垒主机工作机制的分析，可以看出堡垒主机有如下功能特性。

- 堡垒主机自身必须是一个安全系统，从硬件结构到操作系统都必须体现出高可靠性和高安全性的特点。
- 不同的应用层服务是相互独立的，可以动态增加和删除堡垒主机支持的应用层服务，以此适应不同的应用环境。
- 堡垒主机必须具有认证终端用户身份的功能。
- 堡垒主机可以通过设置访问权限确定内部网络中允许外部网络终端访问的网络资源范围。
- 堡垒主机需要详细记录外部网络终端每一次访问内部网络资源所涉及的操作和传输的信息，以便发现和追踪入侵者。

7.4　统一访问控制

网络的发展对网络资源的安全访问提出了新的要求：一是移动性，终端用户不再固定连接在某一个子网上，允许某个用户出现在不同的子网，但拥有相同的访问权限。二是

动态性，终端用户的访问权限是动态变化的，如一台正常的终端允许接入内部网络并访问内部网络资源，一旦确定该终端感染病毒，应立即将该终端和内部网络隔离，另外，有些资源的访问受时间和地点的限制，如敏感数据只允许某个用户在正常办公时间和固定办公地点进行访问，这些都需要动态调整用户的访问权限。三是基于用户，而不是基于终端设置访问权限，同一办公地点可能混杂各种类型的用户，这些用户可能在不同的时间段使用同一终端访问网络资源，显然，当不同用户使用该终端访问网络资源时，该终端的访问权限必须是不同的。一旦需要实现动态安全策略，就无法使用手工配置防火墙的方式，必须由统一的安全控制器通过实时检测用户终端状态、用户终端位置和访问的资源类型动态生成访问控制策略，并将访问控制策略实时地传输到相关的安全设备，如防火墙等。这种通过在网络中设置统一的安全控制器，实施动态访问控制策略的网络资源访问控制系统就是统一访问控制(Unified Access Control，UAC)。

7.4.1 系统结构

采用统一访问控制的网络系统结构如图 7.19 所示，和统一访问控制相关的部件有 UAC 代理、安全控制器和策略执行部件。

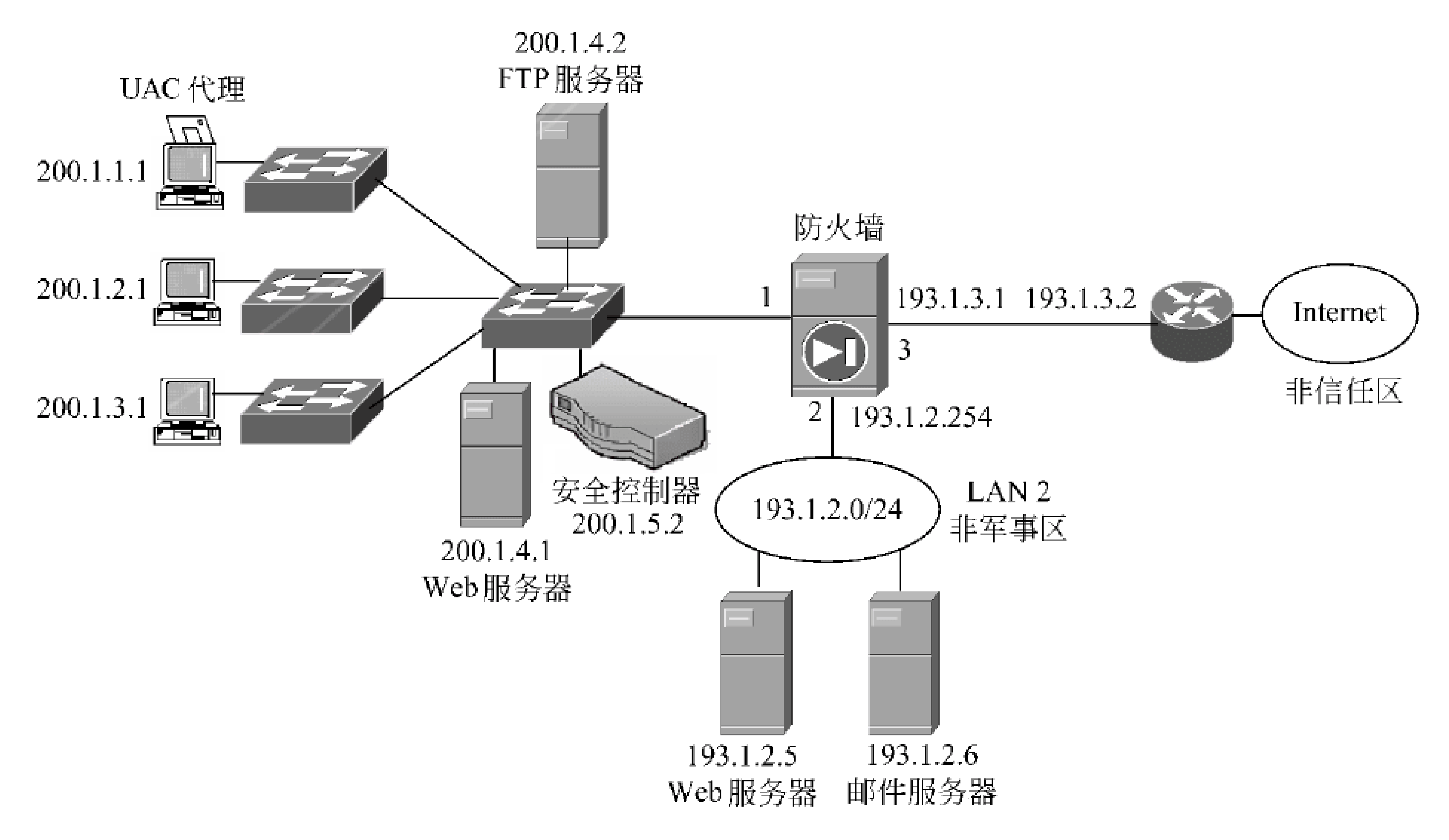


图 7.19 系统结构

1. UAC 代理

UAC 代理是运行在终端上的一个客户软件，和安全控制器构成一个客户、服务器(C/S)系统，它的主要功能如下。

- 向安全控制器提供客户的信用信息，如用户名、口令或相关证书。
- 检测终端的安全状态，如所安装的操作系统和应用系统是否存在漏洞，是否已经下载对应的补丁软件，终端是否安装防病毒软件，系统是否感染病毒等，并及时向安全控制器报告检测结果。

- 检测和设置终端的访问控制策略，如果终端安装个人防火墙，检测个人防火墙的访问控制策略配置，并向安全控制器报告检测结果，也允许安全控制器通过命令修改终端的访问控制策略。

统一访问控制方式下的终端如果需要访问网络中的资源，必须先通过 UAC 代理和安全控制器建立会话，通过会话向安全控制器报告终端的信用信息、安全状态和个人防火墙配置的访问控制策略等，并在上述信息发生变化的情况下，及时报告变化后的信息。在终端访问网络资源期间，UAC 代理和安全控制器之间的会话必须存在。

2. 安全控制器

安全控制器是统一访问控制（UAC）系统的核心，它的主要功能如下：

- 建立统一的访问控制策略库，针对不同用户、终端不同的安全状态定义对应的资源访问策略。
- 及时收集用户的信用信息、终端的安全状态和终端配置的访问控制策略，结合统一的访问控制策略库动态生成类似防火墙等策略执行部件用于控制信息交换的访问控制策略。
- 及时向终端访问资源过程中涉及的策略执行部件推送访问控制策略，并收集策略执行部件检测到的信息流异常情况，根据要求随时调整相关用户的访问权限，并因此重新生成访问控制策略，将其推送到相关策略执行部件。

在某个用户访问网络资源过程中，安全控制器一方面必须维持和该用户终端上运行的 UAC 代理之间的会话，通过会话及时了解该终端的相关信息和状态，另一方面必须维持和用户访问网络资源过程涉及的策略执行部件之间的会话，通过会话随时了解用户访问网络资源过程中产生的信息流模式，在一切正常的情况下，允许用户访问网络资源过程正常进行；否则，立即通过向用户访问网络资源过程涉及的策略执行部件推送命令，终止该次访问过程。

3. 策略执行部件

策略执行部件是根据安全控制器动态生成的访问控制策略控制用户终端对网络资源的访问过程的部件，它的主要功能如下：

- 建立、维持和安全控制器之间的会话，通过会话接收安全控制器为其制定的访问控制策略，随时通过会话向安全控制器汇报检测到的信息流异常情况。
- 根据安全控制器为其制定的访问控制策略调整安全机制，这些安全机制包括分组过滤器、信息流优先级设置和流量管制等。
- 根据自己位于网络的位置（作为接入设备位于网络边缘，或作为网络核心控制设备）选择对应的建立、维持和安全控制器之间的会话的方法及用于实现访问控制策略的安全机制。

7.4.2 实现原理

1. 系统配置

实现 UAC 的系统配置如图 7.20 所示，它的主要特点一是接入交换机 S_1、S_2 和 S_3 对接入终端用 802.1X 进行身份认证，并根据认证结果动态配置连接用户终端的端口的

VLAN，二是安全控制器作为 802.1X 的认证服务器，一方面完成对接入用户的身份认证，另一方面根据用户终端 UAC 代理通过 EAP 发送给它的终端安全状态和配置的安全策略库确定接入终端的端口的 VLAN，并通过 EAP 将端口 VLAN 配置信息发送给接入交换机。接入交换机 S_1、S_2 和 S_3 的 VLAN 配置和核心交换机 S_4 的 VLAN 配置如表 7.3 所示，如此配置 VLAN 的主要目的一是创建 VLAN 1～VLAN 7，二是构建防火墙端口 1 至这些 VLAN 的交换路径。

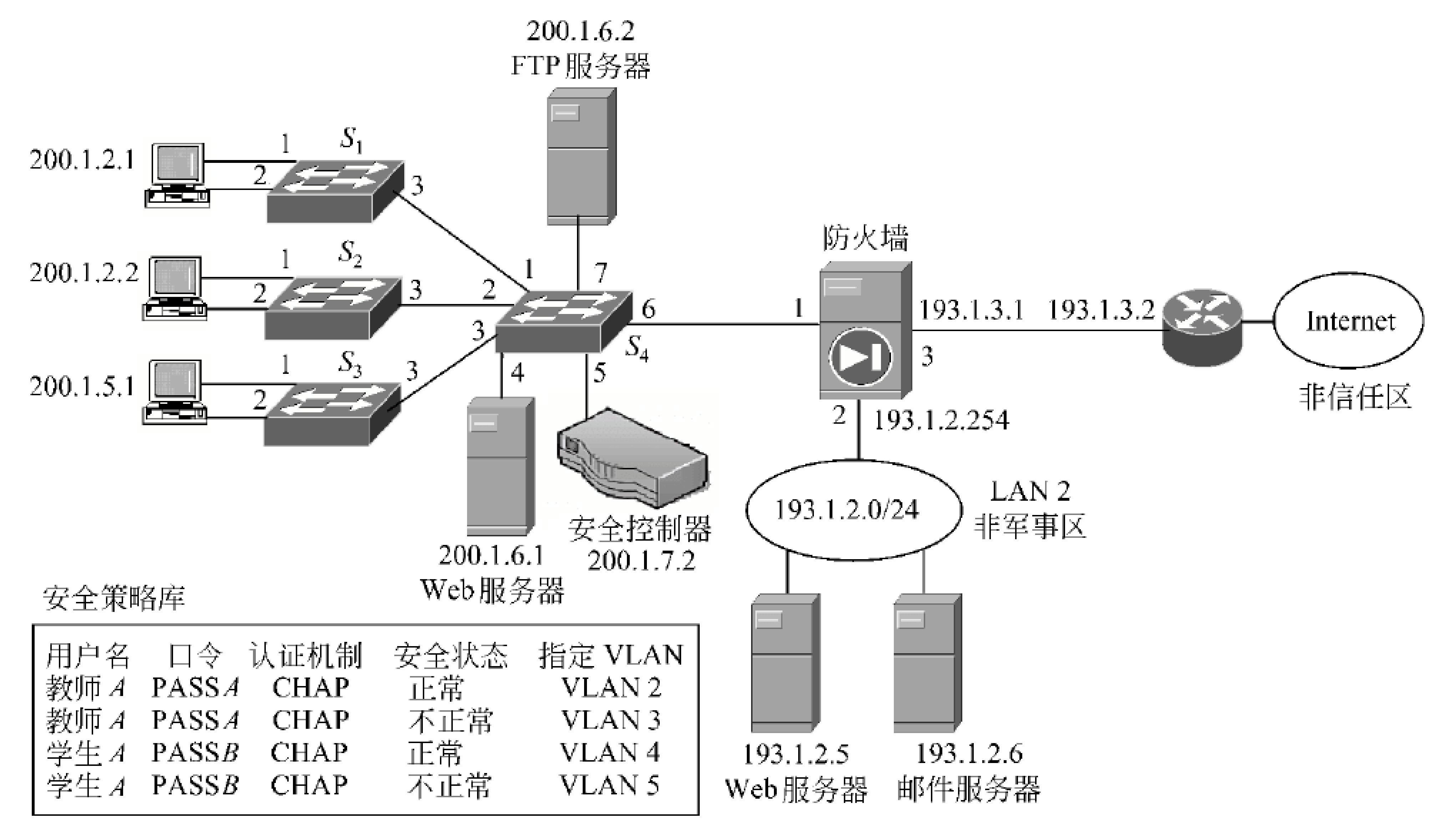


图 7.20 UAC 系统配置

表 7.3 VLAN 配置表

VLAN	非标记端口	标记端口
动态配置	$S_{1.1}$、$S_{1.2}$、$S_{2.1}$、$S_{2.2}$、$S_{3.1}$、$S_{3.2}$	
VLAN 1		$S_{1.3}$、$S_{2.3}$、$S_{3.3}$、$S_{4.1}$、$S_{4.2}$、$S_{4.3}$、$S_{4.6}$
VLAN 2		$S_{1.3}$、$S_{2.3}$、$S_{3.3}$、$S_{4.1}$、$S_{4.2}$、$S_{4.3}$、$S_{4.6}$
VLAN 3		$S_{1.3}$、$S_{2.3}$、$S_{3.3}$、$S_{4.1}$、$S_{4.2}$、$S_{4.3}$、$S_{4.6}$
VLAN 4		$S_{1.3}$、$S_{2.3}$、$S_{3.3}$、$S_{4.1}$、$S_{4.2}$、$S_{4.3}$、$S_{4.6}$
VLAN 5		$S_{1.3}$、$S_{2.3}$、$S_{3.3}$、$S_{4.1}$、$S_{4.2}$、$S_{4.3}$、$S_{4.6}$
VLAN 6	$S_{4.4}$、$S_{4.7}$	$S_{4.6}$
VLAN 7	$S_{4.5}$	$S_{4.6}$

VLAN 对应的子网地址如下所示：

VLAN 1：200.1.1.0/24，VLAN 2：200.1.2.0/24，VLAN 3：200.1.3.0/24，VLAN 4：200.1.4.0/24

VLAN 5：200.1.5.0/24，VLAN 6：200.1.6.0/24，VLAN 7：200.1.7.0/24

VLAN 1 对应管理员区，如果是教师终端且终端安全状态正常接入 VLAN 2，如果是教师终端但终端安全状态不正常接入 VLAN 3，同样，如果是学生终端且终端安全状态正常接入 VLAN 4，如果是学生终端但终端安全状态不正常接入 VLAN 5，安全状态正常是指终端安装了防病毒软件，安装了针对终端所使用的操作系统漏洞的补丁软件，系统没有感染病毒等；否则，表明终端的安全状态不正常。一旦终端的安全状态不正常，一方面需要降低用户的权限，如教师 *A* 在终端安全状态不正常的情况下，对 FTP 服务器的访问权限由读写（FTP 服务）降为只能读（FTP GET 服务）。另一方面，为了防止终端在感染病毒的情况下发起对其他区中终端的拒绝服务攻击，对安全状态不正常的终端访问其他区的流量进行管制，因此，在 VLAN 3 和 VLAN 5 的输出方向上设置如下管制器：

VLAN 3 输出方向　源 IP 地址＝200.1.3.0/24　目的 IP 地址＝0.0.0.0　平均速率＝2Mb/s，突发性数据长度＝32KB。

VLAN 5 输出方向　源 IP 地址＝200.1.5.0/24　目的 IP 地址＝0.0.0.0　平均速率＝1Mb/s，突发性数据长度＝16KB。

将流出 VLAN 3 的流量控制在平均传输速率为 2Mb/s，最大持续传输的数据长度为 32KB。流出 VLAN 5 的流量控制在平均传输速率为 1Mb/s，最大持续传输的数据长度为 16KB。

为防火墙配置的访问控制策略如下：

（1）从教师区 *A* 到服务器区　源 IP 地址＝200.1.2.0/24　目的 IP 地址＝200.1.6.1/32　HTTP GET 服务；

（2）从教师区 *A* 到服务器区　源 IP 地址＝200.1.2.0/24　目的 IP 地址＝200.1.6.2/32　FTP 服务；

（3）从教师区 *B* 到服务器区　源 IP 地址＝200.1.3.0/24　目的 IP 地址＝200.1.6.1/32　HTTP GET 服务；

（4）从教师区 *B* 到服务器区　源 IP 地址＝200.1.3.0/24　目的 IP 地址＝200.1.6.2/32　FTP GET 服务；

（5）从学生区 *A* 到服务器区　源 IP 地址＝200.1.4.0/24　目的 IP 地址＝200.1.6.1/32　HTTP GET 服务；

（6）从学生区 *A* 到服务器区　源 IP 地址＝200.1.4.0/24　目的 IP 地址＝200.1.6.2/32　FTP GET 服务；

（7）从学生区 *B* 到服务器区　源 IP 地址＝200.1.5.0/24　目的 IP 地址＝200.1.6.1/32　HTTP GET 服务；

（8）从学生区 *B* 到服务器区　源 IP 地址＝200.1.5.0/24　目的 IP 地址＝200.1.6.2/32　FTP GET 服务。

为安全控制器设置图 7.21 所示的安全策略库，安全策略库中为每一个注册用户指定认证机制，同时根据用户属性（学生或教师）和用户终端的安全状态（正常或不正常）确定用户终端所属的 VLAN。安全控制器根据安全策略库和用户终端状态确定用户终端所属的 VLAN，防火墙访问控制策略根据用户终端所属的 VLAN 确定终端访问网络资源（Web 服务器和 FTP 服务器）的权限，同时，防火墙为 VLAN 3 和 VLAN 5 配置的流量管

制器对流出 VLAN 3 和 VLAN 5 的流量进行限制，以此对接入用户访问网络资源的过程实施控制。

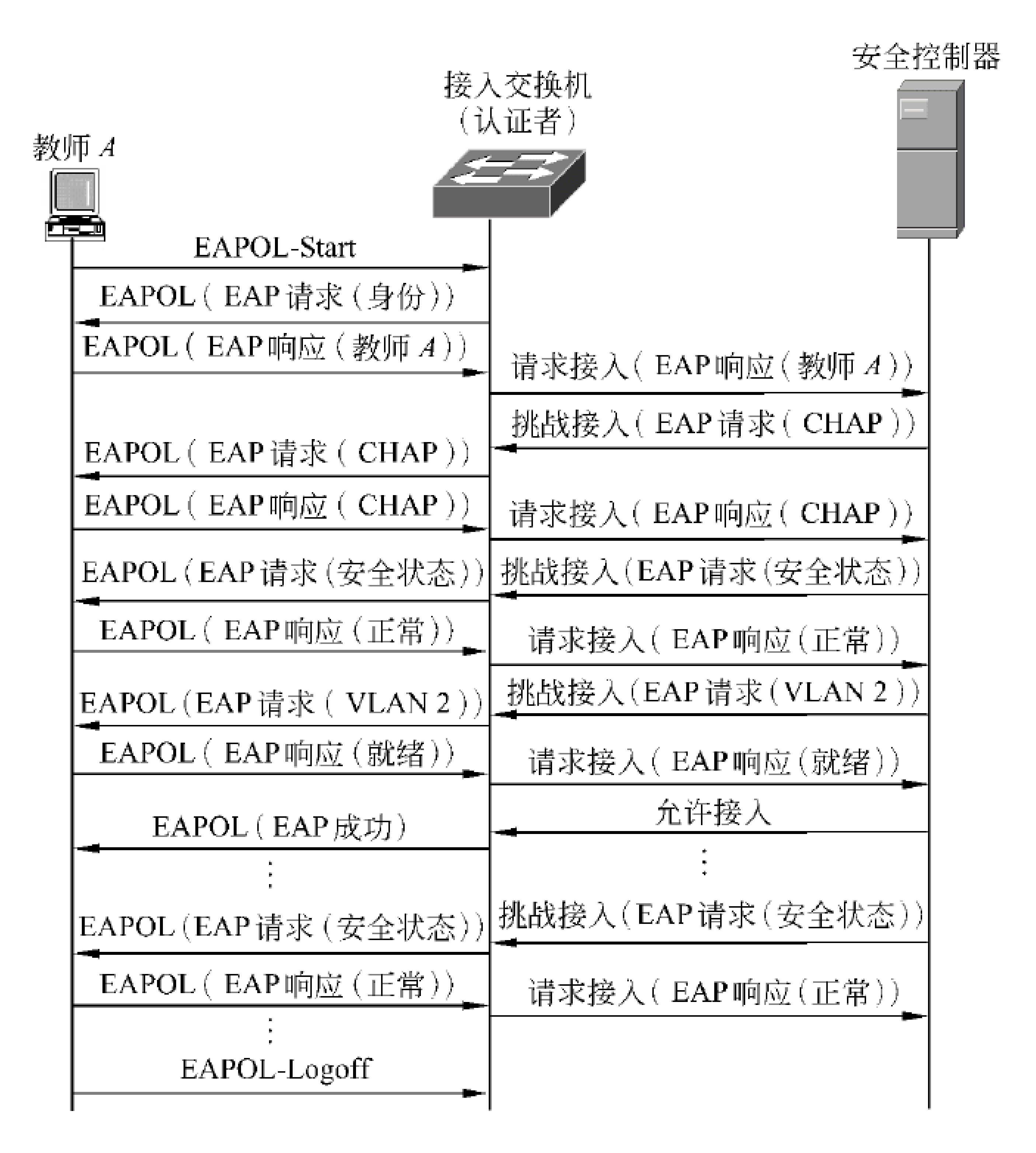


图 7.21 UAC 工作过程

2. UAC 工作过程

当教师 A 将终端接入某个接入交换机端口（如接入交换机端口 1）后，启动 UAC 代理，UAC 代理通过向接入交换机发送 EAPOL-Start 报文开始 802.1X 认证过程，EAPOL-Start 是 802.1X 定义的报文类型，用于由用户发起 802.1X 认证过程的情况。接入交换机接收到用户终端发送的 EAPOL-Start 报文后，开始 802.1X 认证过程。接入交换机作为认证者首先要求用户终端提供用户名，并将用户终端提供的用户名通过 RADIUS 请求接入报文发送给安全控制器。接入交换机都是可管理设备，需要分配管理地址，一般情况下，将内网中的所有网络设备的管理地址配置成同一子网地址，而且，在为防火墙配置的访问控制策略中允许管理员访问网络设备，允许接入交换机和安全控制器交换 RADIUS 报文。安全控制器接收到用户名后，检测安全策略库，确定用户教师 A 的认证机制：CHAP，向教师 A 发送随机数 challenge，教师 A 根据口令和随机数 challenge 计算出认证结果，将认证结果回送给安全控制器，安全控制器对认证结果进行验证。一旦通过验证，表明用户身份得到确认。随后，安全控制器向用户发送安全状态查询请求，UAC 代理对查询请求中列出的检测项目逐个检测，并将检测结果回送给安全控制器，安全控制器根据用户终端的安全状态确定终端所连接的接入交换机端口的 VLAN，向接入

交换机发送配置端口 VLAN 的命令。安全控制器通过 RADIUS 报文中设备专有属性字段发送接入交换机的配置命令，因此，在基本配置阶段，必须在安全控制器和接入交换机之间就配置命令类型、格式和功能达成一致。接入交换机接收到包含配置端口 VLAN 命令的 RADIUS 报文后，将指定端口作为非标记端口划分到指定 VLAN 中，同时向用户终端通报这一配置结果。用户终端通过发送就绪报文对安全控制器的配置结果予以确认，安全控制器通过允许接入报文结束对接入用户的认证和配置过程。

用户终端完成认证和配置过程后，启动 DHCP 过程获得和终端所属 VLAN（VLAN 2）对应的 IP 地址和子网掩码（如 192.1.2.1/24）、默认网关地址（192.1.2.254）等，然后开始对网络资源的访问过程，防火墙根据访问控制策略（1）和（2）对教师 *A* 访问 Web 服务器和 FTP 服务器的过程进行控制。

7.4.3　应用实例

图 7.20 所示的系统配置解决统一接入问题的前提是接入交换机支持 802.1X 和动态 VLAN 配置，安全控制器能够通过 RADIU 报文中设备专有属性字段传输的配置端口 VLAN 命令对接入交换机的端口动态划分 VLAN。解决的问题是内网中通过以太网接入的用户的移动性和基于用户设置访问权限的问题。如果需要解决用户更广泛范围内的移动性，如通过外网访问内网网络资源的问题，图 7.20 所示的系统配置是无法实现的。

1. 系统配置

图 7.22 是动态实现教师 *A* 通过外网访问内网资源的系统配置，防火墙初始配置的访问控制策略只允许非信任区中的终端访问非军事区中的服务器，因此，当连接在非信任区的教师 *A* 希望通过登录安全控制器，获得访问信任区中 Web 和 FTP 服务器的权限时，

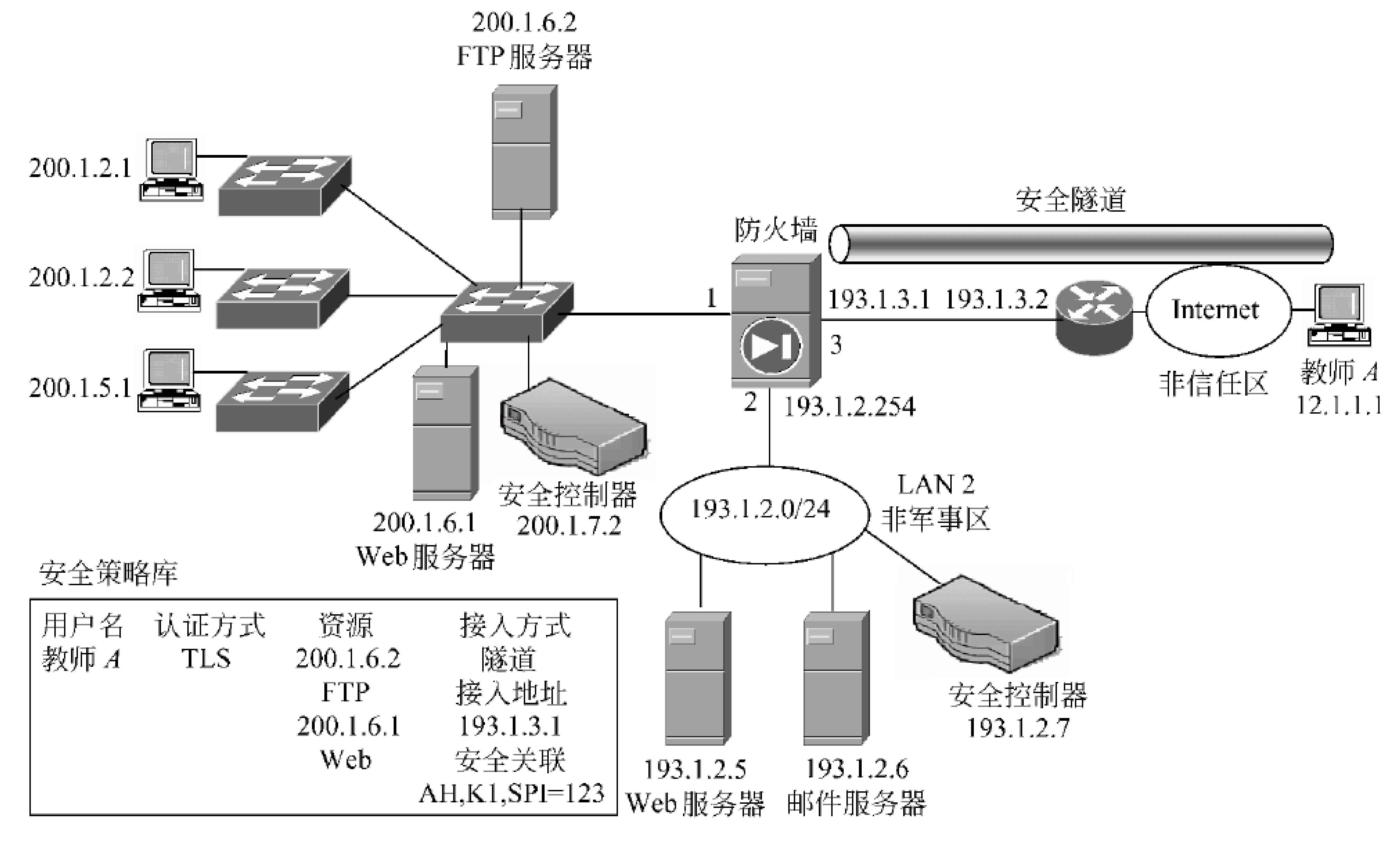


图 7.22　实现远程访问控制的 UAC 系统配置

一是必须在非军事区中配置安全控制器，二是通过登录 Web 服务器的方式完成教师 *A* 的身份认证和权限鉴别。

防火墙初始配置的和教师 *A* 登录安全控制器有关的访问控制策略如下：

从非信任区到非军事区　源 IP 地址＝0.0.0.0　目的 IP 地址＝193.1.2.7/32 HTTPS GET 服务。

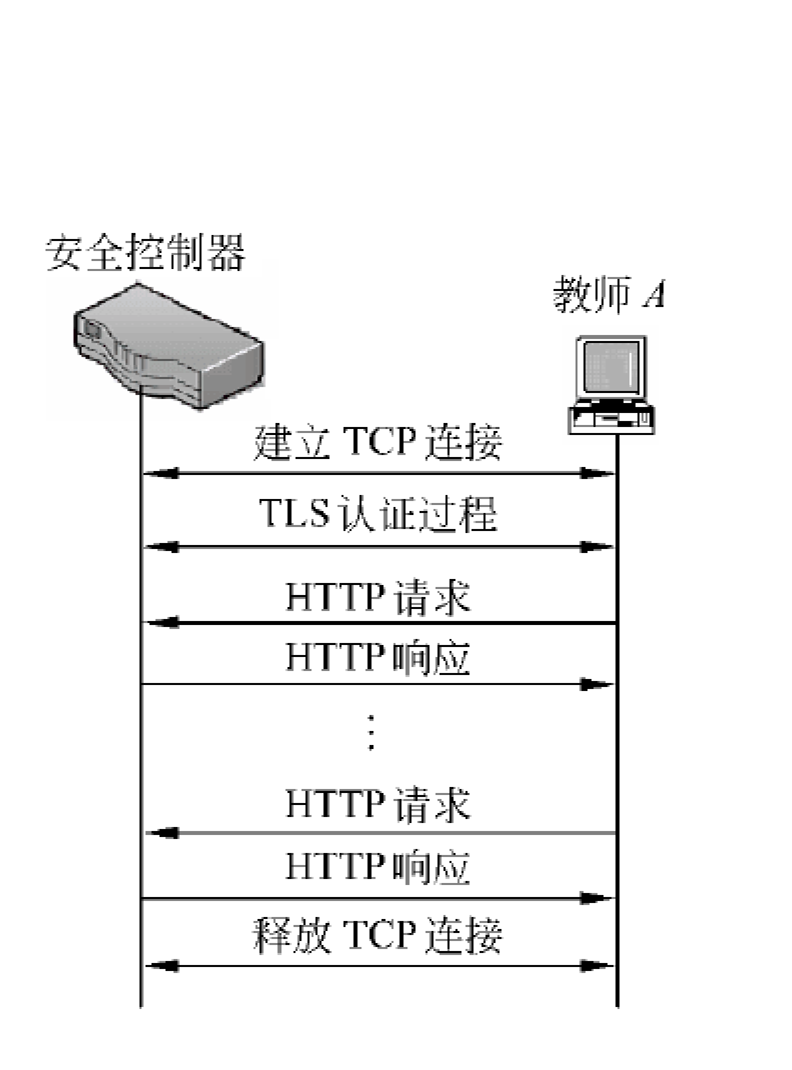
安全控制器和非信任区中的终端之间通过 TLS 完成相互身份认证，教师 *A* 允许访问的资源是 IP 地址分别为 200.1.6.2 和 200.1.6.1 的 FTP 和 Web 服务器。由于安全控制器完成对教师 *A* 的身份认证后，建立教师 *A* 和其 IP 地址的绑定，防火墙通过 IP 地址来鉴别来自教师 *A* 的 IP 分组，但由于存在源 IP 地址欺骗攻击，黑客可能通过盗用教师 *A* 的 IP 地址对内网中的 FTP 和 Web 服务器实施攻击。为了避免发生这种情况，当教师 *A* 访问内网中的 FTP 和 Web 服务器时，教师 *A* 和防火墙连接非军事区的端口之间先建立隧道和安全关联，用 IPSec AH 鉴别 IP 分组源终端的真实性。

2. 身份认证和访问控制策略动态配置过程

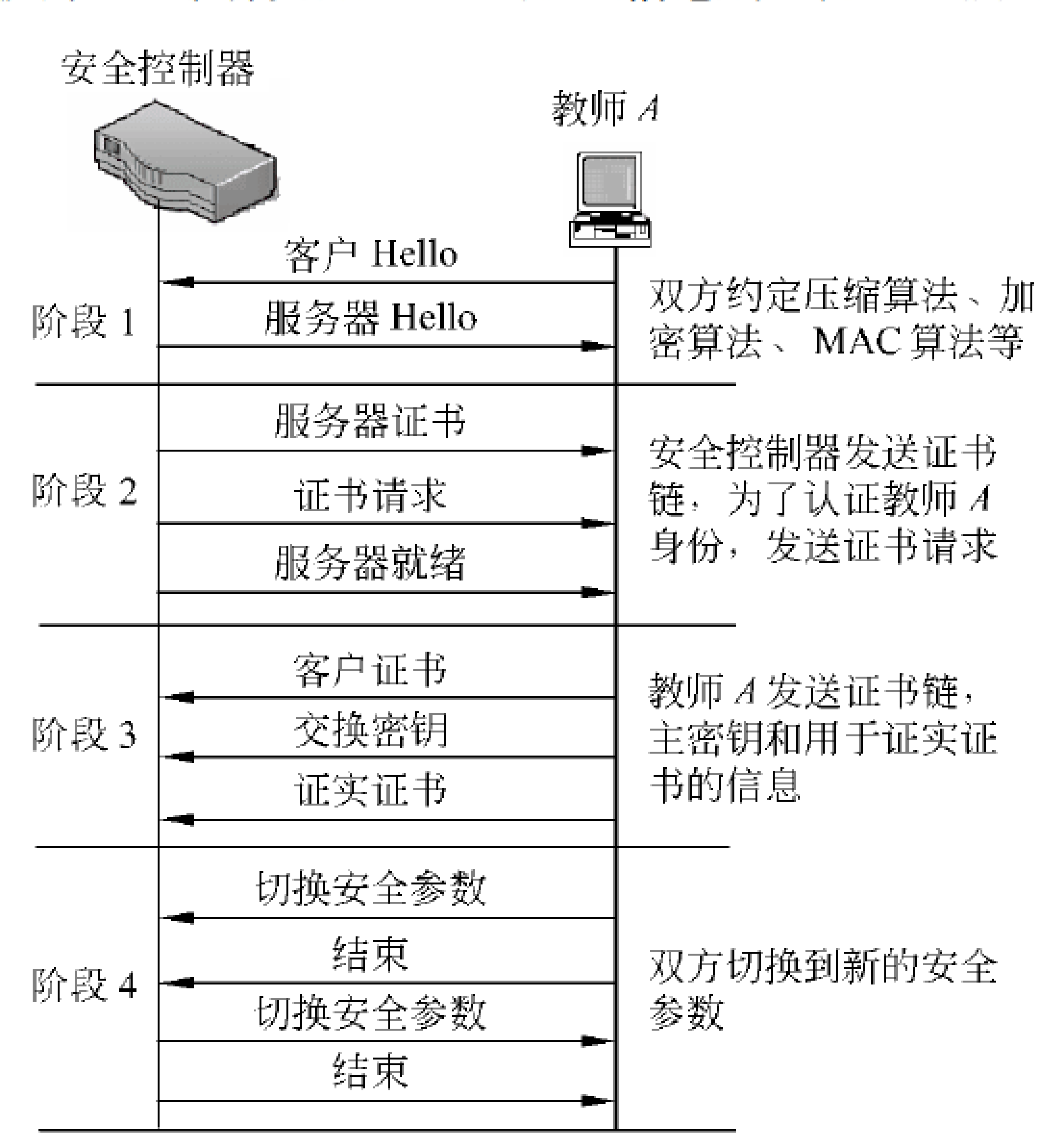
教师 *A* 访问内网服务器资源前，必须启动 UAC 代理登录安全控制器，如图 7.23 所示，该过程一是完成相互身份认证，由安全控制器将教师 *A* 和 IP 地址 12.1.1.1 绑定在一起。二是教师 *A* 通过 HTTP 和安全控制器交换安全状态信息。

安全控制器在完成对教师 *A* 身份认证和确定教师 *A* 终端安全状态正常后，开始根据安全策略库中配置的信息动态配置防火墙的访问控制策略和防火墙与教师 *A* 终端有关 IPSec 的安全参数。

首先由安全控制器通过 HTTP 向教师 *A* 终端发送 IPSec 配置信息，如表 7.4 所示。




(a) 教师 *A* 和安全控制器交换信息过程



(b) TLS 相互认证过程

图 7.23　教师 *A* 登录安全控制器过程

配置信息要求对源和目的IP地址分别为12.1.1.1/32和200.1.6.0/30的IP分组进行IPSec处理，IPSec采用隧道模式，隧道两端地址分别为12.1.1.1和193.1.3.1，通过AH保证IP分组的完整性。和教师*A*终端至隧道另一端的安全关联有关的安全参数包括SPI(123)、认证算法(HMAC-MD5-96)和认证密钥(KEY)，这些配置信息必须保证安全传输；否则，隧道的安全传输特性无法保证。由于通过TLS握手协议完成安全控制器和教师*A*双向身份认证时已经分配了共享密钥，因此，通过将HTTP报文封装成TLS记录报文实现安全控制器和教师*A*终端之间的双向安全传输。

表7.4 教师A终端IPSec配置

IP分组分类信息		隧道信息		安全关联			
源地址	目的地址	端地址1	端地址2	SPI	安全协议	认证算法	认证密钥
12.1.1.1/32	200.1.6.0/30	12.1.1.1	193.1.3.1	123	AH	HMAC-MD5-96	KEY

同样，安全控制器向防火墙发送IPSec配置信息和允许教师*A*访问内网服务器资源的访问控制策略。IPSec配置信息和教师*A*终端相似，如表7.5所示。对防火墙动态配置的访问控制策略如下：

(1) 从非信任区到信任区　源IP地址=12.1.1.1/32　目的IP地址=200.1.6.1/32 HTTP GET服务，非信任区接口采用IPSec AH。

(2) 从非信任区到信任区　源IP地址=12.1.1.1/32　目的IP地址=200.1.6.2/32 FTP GET服务，非信任区接口采用IPSec AH。

表7.5 防火墙IPSec配置

IP分组分类信息		隧道信息		安全关联			
源地址	目的地址	端地址1	端地址2	SPI	安全协议	认证算法	认证密钥
200.1.6.0/30	12.1.1.1/32	193.1.3.1	12.1.1.1	123	AH	HMAC-MD5-96	KEY

访问控制策略允许外网中IP地址为12.1.1.1/32的终端发起对内网中IP地址为200.1.6.1服务器的HTTP GET访问过程，IP地址为200.1.6.2服务器的FTP GET访问过程，但访问过程中涉及的TCP报文必须以IPSec AH封装格式在防火墙和教师*A*终端之间传输。安全控制器和防火墙之间需要通过专用安全传输协议实现配置信息和状态信息的双向安全传输。

无论是教师*A*终端配置的IPSec信息，还是防火墙配置的IPSec信息和访问控制策略都是在教师*A*登录安全控制器期间且教师*A*终端安全状态正常的情况下才有效，一旦教师*A*退出安全控制器或者教师*A*终端安全状态变成不正常，安全控制器将立即删除这些配置。

3. 教师A终端访问内网资源过程

教师*A*通过UAC代理成功登录安全控制器后，可以启动对内网服务器资源的访问过程，当教师*A*访问内网中IP地址为200.1.6.1的Web服务器时，教师*A*终端和内网

Web 服务器之间进行图 7.6 所示的信息交换过程，但由于教师 *A* 终端发送的 IP 分组符合 IPSec 配置中的 IP 分组分类条件，这些 IP 分组需要先进行 IPSec 处理，如图 7.24 所示。IPSec AH 格式的 IP 分组经过外网传输后，到达防火墙，由于匹配防火墙配置的安全关联（SPI＝123、目的 IP 地址＝193.1.3.1、安全协议＝AH），防火墙根据相关安全参数（认证算法＝HMAC-MD5-96、认证密钥＝KEY）对 IPSec AH 格式的 IP 分组进行完整性检测，在完整性检测正确的情况下，分离出内层 IP 分组，然后根据会话表和访问控制策略对内层 IP 分组进行转发许可控制。根据访问控制策略，对从非信任区接收到的 IP 分组，如果封装形式不是 IPSec AH 格式，即使源和目的 IP 地址及所请求的服务符合访问控制策略或会话表中信息，也不能转发给内网中的服务器。同样，防火墙对于从非信任区接口转发出去的 IP 分组，如果 IP 分组的源和目的地址符合 IPSec 配置中的 IP 分组分类条件，这些 IP 分组需要先进行 IPSec 处理。

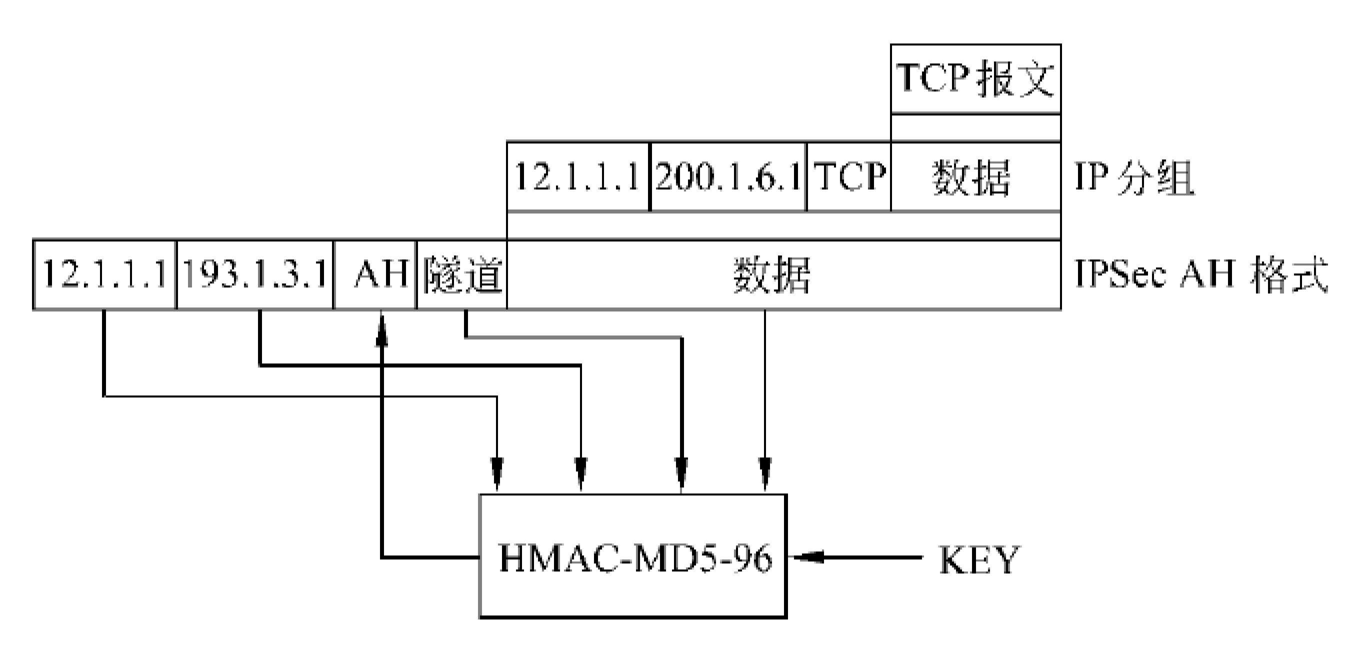


图 7.24 终端封装 TCP 报文过程

由于终端发送 IP 分组时，先将 IP 分组封装成图 7.24 所示的 IPSec 格式，而计算 AH 中的认证数据时需要认证密钥 KEY，认证密钥 KEY 只有终端至防火墙的安全关联的双方（终端和防火墙）才能掌握，这就意味着只有终端才能产生正确的认证数据，防火墙能够鉴别正确的认证数据且只转发认证数据正确的 IPSec AH 格式中的内层 IP 分组。由于黑客无法获得认证密钥 KEY，因而无法产生防火墙能够鉴别的认证数据，导致黑客伪造教师 *A* 终端地址的 IP 分组被防火墙丢弃。同样，黑客也无法篡改内网 Web 服务器发送给终端的 IP 分组。

习 题

7.1 有状态分组过滤器和无状态分组过滤器有什么本质区别？

7.2 个人防火墙的主要功能是什么？这些功能包含在哪一类网络防火墙中？

7.3 电路层网关和应用层网关的主要功能是什么？为什么说目前的有状态分组过滤器包含了这两类网关的主要功能？

7.4 堡垒主机与电路层网关和应用层网关之间有什么关系？它和有状态分组过滤器的区别是什么？

7.5 有一个网络如图 7.25 所示，如果要禁止子网 1 和子网 2 之间的信息传输，如何

设置无状态分组过滤器？如果只允许子网 1 内终端访问子网 2 内 Web 服务器，而不允许其他信息传输过程，如何设置无状态分组过滤器？

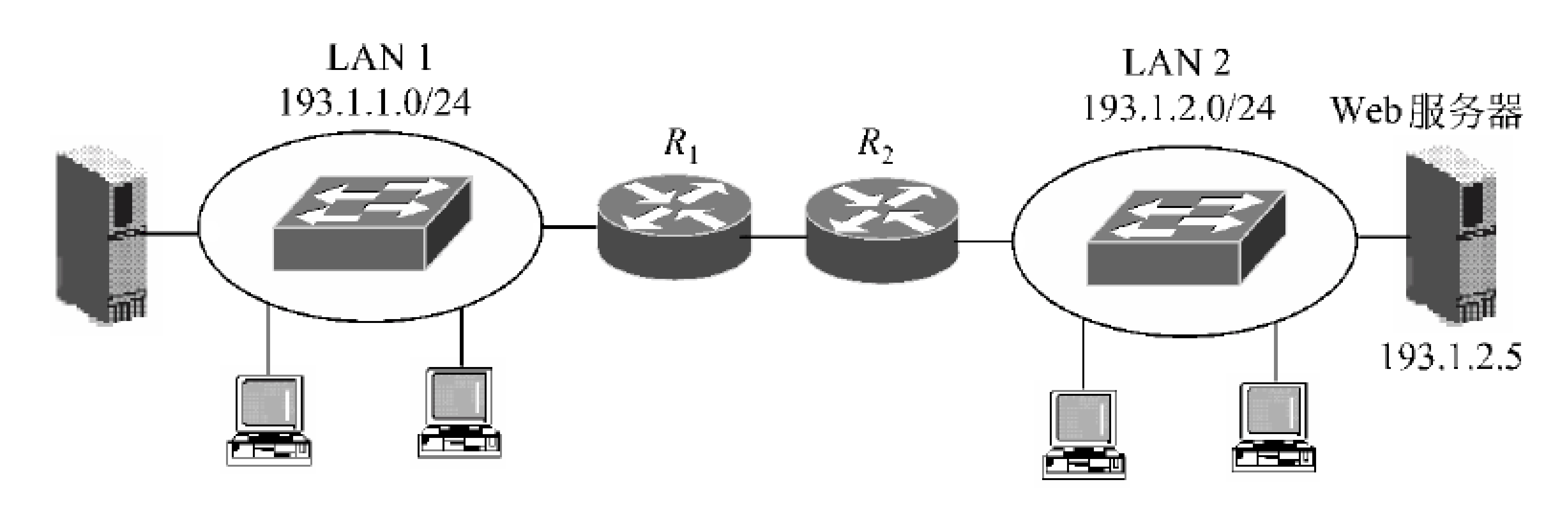


图 7.25　题 7.5 图

7.6　为什么有状态分组过滤器能更精确地控制信息流动，用有状态分组过滤器实现习题 7.5 的功能，并说明优于无状态分组过滤器的地方。

7.7　如何理解有状态分组过滤器访问控制策略中的服务。

7.8　精确解释访问控制策略：

从信任区到非信任区　源 IP 地址＝193.1.1.0/24　目的 IP 地址＝0.0.0.0　HTTP＋FTP GET 服务。

各个部分的含义。

7.9　网络结构如图 7.26 所示，内部网络被分成四个子网，分别分配 IP 地址 200.1.1.0/24、200.1.2.0/24、200.1.3.0/24 和 200.1.4.0/24，请制定符合下列访问策略的访问控制策略。

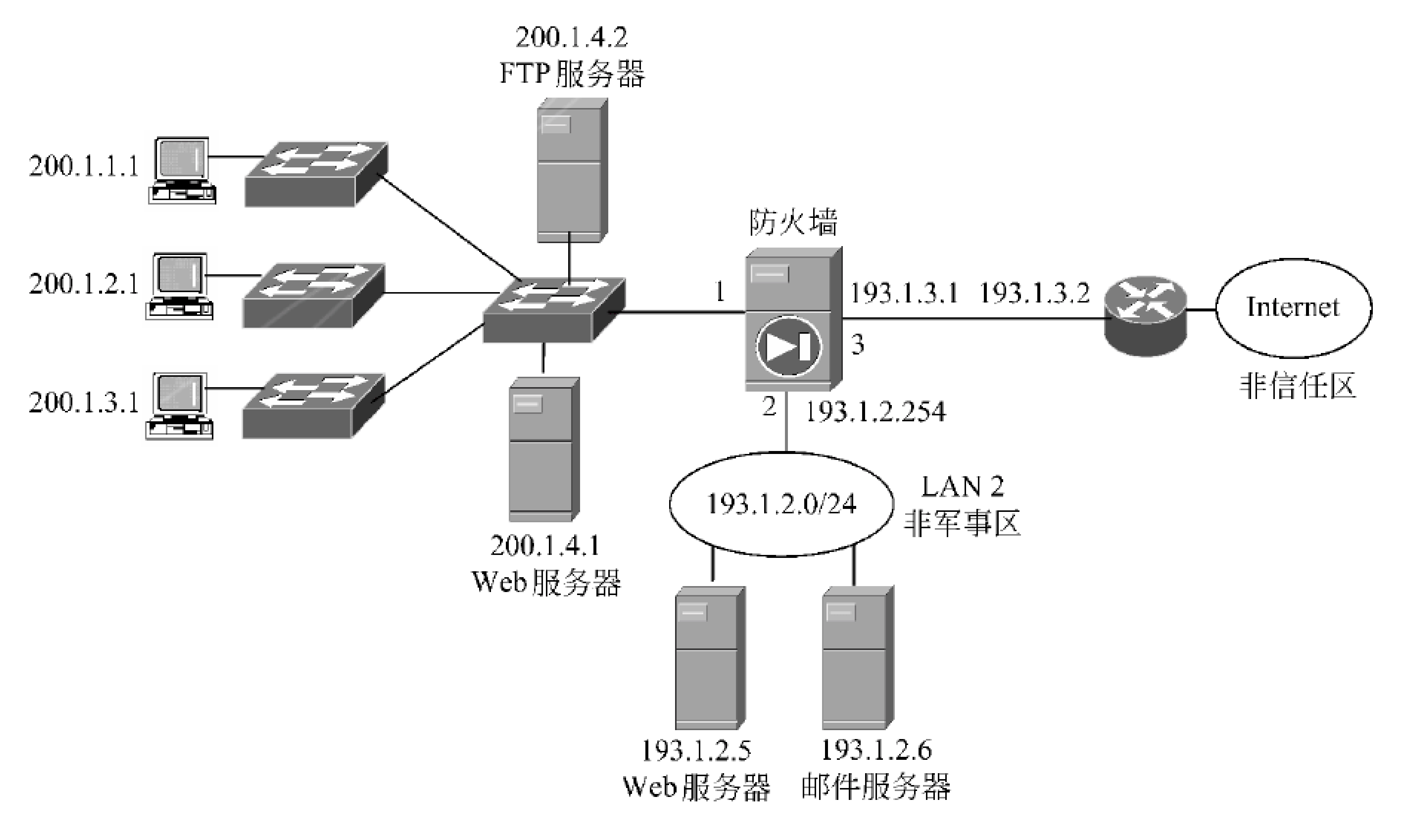


图 7.26　题 7.9 图

- 允许属于 VLAN 1 的终端访问内部服务器、非军事区服务器和 Internet 中的 Web 和 FTP 服务器；

• 允许属于 VLAN 2 的终端访问内部网络服务器和非军事区中的 Web 服务器；
• 允许属于 VLAN 3 的终端访问内部网络服务器。

并根据访问控制策略解释防火墙阻止属于 VLAN 3 的终端访问非军事区中服务器的工作机制。

7.10 有状态分组过滤器能否通过制定访问控制策略实现基于用户的访问控制过程。

7.11 网络结构如图 7.27 所示，堡垒主机能否基于用户对外部终端访问内部网络资源过程实施控制？解释访问控制机制。

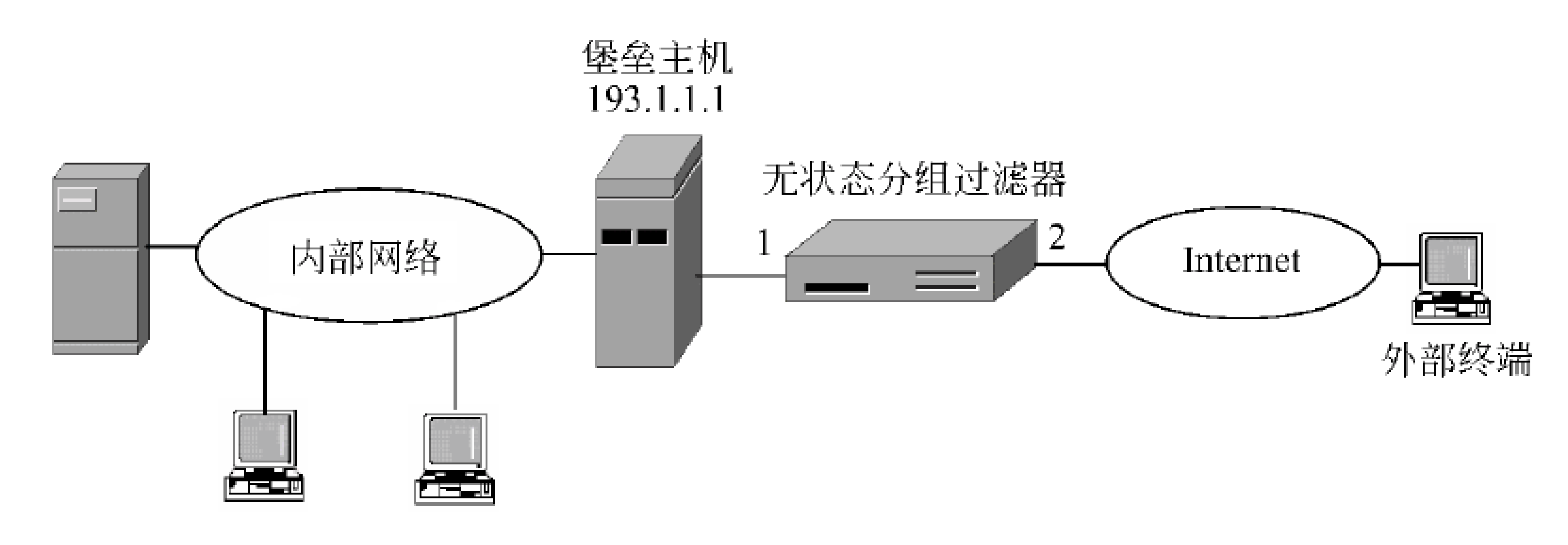


图 7.27 题 7.11 图

7.12 网络结构如图 7.27 所示，堡垒主机能否控制内部网络各子网间的信息交换过程？根据答案解释原因。

7.13 图 7.27 中的堡垒主机和图 7.26 中的有状态分组过滤器(防火墙)有什么本质区别？

7.14 提出统一访问控制的起因是什么？统一访问控制实现哪些功能？

7.15 统一访问控制系统有哪些基本构件，它们的主要功能是什么？

7.16 将图 7.26 所示的网络结构改为统一访问控制系统，正常访问控制策略和题 7.9 相同，但要求：

• 一旦检测到属于 VLAN 1 和 VLAN 2 的终端感染病毒，立即取消访问内部网络服务器的权限；
• 一旦检测到属于 VLAN 1 和 VLAN 2 的终端发起对非军事区中服务器的 SYN 泛洪攻击，立即取消访问非军事区中服务器的权限；
• 一旦检测到属于 VLAN 3 的终端感染病毒，立即关闭交换机连接该终端的端口。

给出统一控制系统中各构件的配置信息，使其具有动态调整访问控制策略的功能。

第8章 入侵防御系统

CHAPTER

8.1 入侵防御系统概述

随着Internet和人们的生活息息相关，网络安全问题日益严重，非法访问、拒绝服务攻击（DoS）、非法代码等危害网络安全的活动越来越多，由于TCP/IP网络体系结构的安全性的先天不足，使得网络安全问题的解决成为一件十分困难的事情，网络安全威胁的多样性决定没有单一技术可以解决所有安全问题，解决网络安全问题必须构建网络安全体系，在网络体系结构中的每一层设置多种安全技术，并将这些分布在各层的安全技术融合为一个有机的整体。

第7章讨论了防火墙技术，防火墙是一种设置在网络边界，有效控制内网和外网之间信息交换的设备，如通过配置访问控制策略，可以将外网对非军事区中的资源的访问权限设置为只允许读取Web服务器中的Web页面和FTP服务器中的文件。但外网对内网中终端实施的攻击往往通过防火墙访问控制策略所允许的信息交换过程完成，如通过内网终端访问外网Web服务器时或通过内网终端接收的邮件安装非法代码，因此，在网络威胁多样化的今天，防火墙已经无法防止来自外网的全部攻击。除了来自外网的攻击，内网中安装了非法代码的终端，或内网中不怀好意的用户也有可能发起对内网中其他终端或服务器的攻击，由于这种攻击涉及的信息交换过程不需要经过防火墙，无法由防火墙对这类攻击进行有效防护，因此，需要增加一种能够有效检测传输的信息是否异常并对异常信息的传输过程进行干预，或者能够确定对主机资源的访问是否合法并对非法访问进行管制的设备，这种设备就是入侵防御系统（Intrusion Prevention System，IPS），异常信息是指用于实施攻击的信息、信息内容和指定应用不符的信息或包含非法代码的信息，对主机资源的非法访问是指违背正常访问原则，或是可能对主机系统造成破坏的访问操作。

8.1.1 入侵防御系统分类

从图8.1可以看出，入侵防御系统分为主机入侵防御系统（Host

Intrusion Prevention System，HIPS）和网络入侵防御系统（Network Intrusion Prevention System，NIPS）两大类，网络入侵防御系统主要用于检测流经网络某段链路的信息流，而主机入侵防御系统主要用于检测到达某台主机的信息流、监测对主机资源的访问操作。网络主要由三部分组成：主机、结点和链路。主机包括终端和服务器，是网络资源的主要载体；结点用于路由、转发分组；链路用于实现结点间通信，因此，这三部分都有可能成为黑客攻击的目标。通过网络入侵防御系统实现对主机的保护是困难的，一是网络入侵防御系统只能捕获单段链路的信息流，无法对流经网络各段链路的所有信息流进行检测。二是网络入侵防御系统是无法检测出所有已知或未知的攻击。三是不同的主机配置，如不同的操作系统、应用服务器平台，对攻击的定义不同。四是当主机是攻击目标时，攻击动作在主机展开，主机是判别接收到的信息是否是攻击信息的合适之处。因此，对主机的有效保护主要通过主机入侵防御系统实现，由于主机是网络资源的主要载体，因此，主机入侵防御系统的重要性不言而喻。

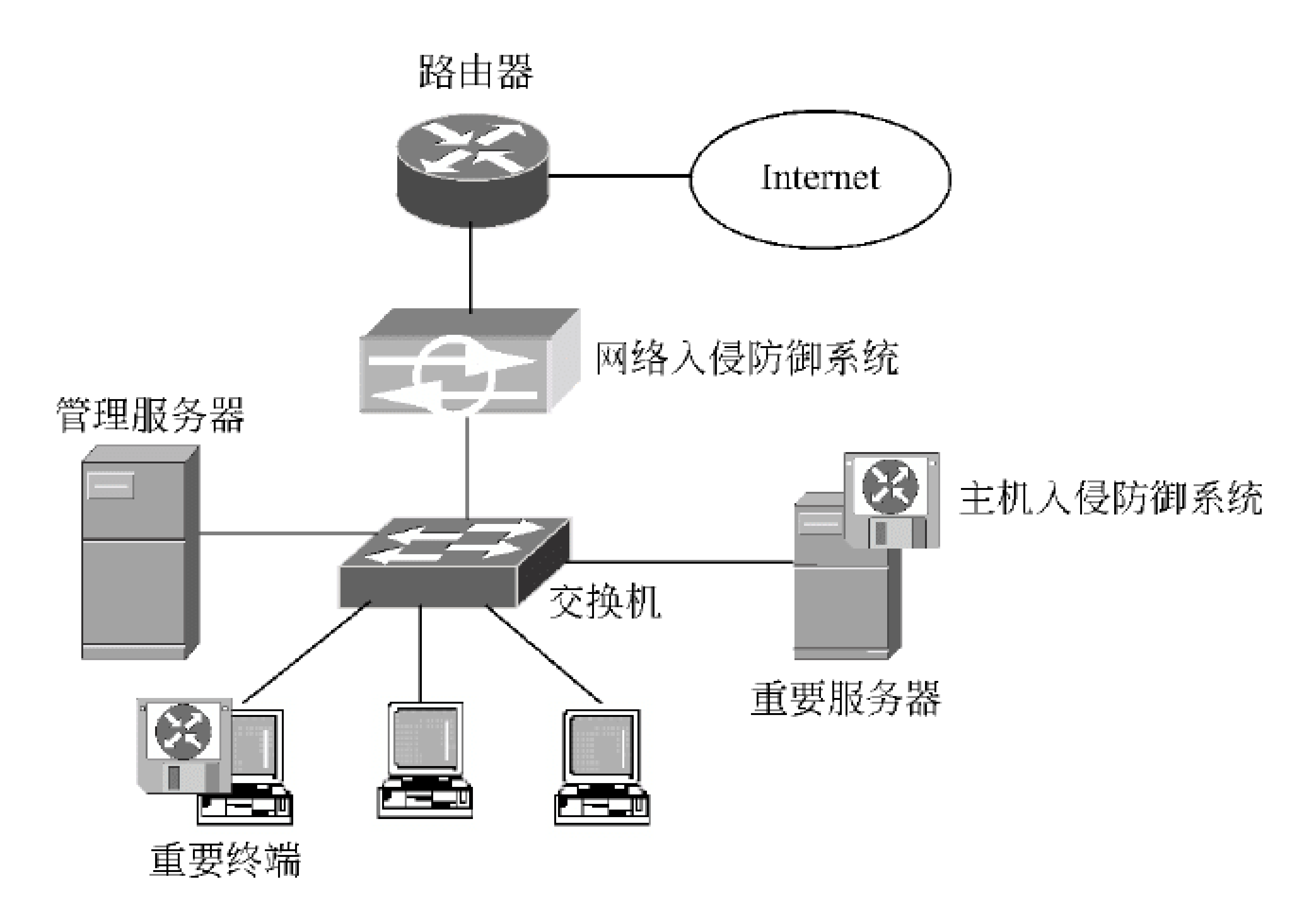


图 8.1 入侵防御系统应用模式

1. 主机入侵防御系统

主机入侵防御系统对所有进入主机的信息进行检测，对所有和主机建立的 TCP 连接进行监控，对所有发生在主机上的操作进行管制，它具有如下特有的功能。

1）有效抵御非法代码攻击

抵御非法代码攻击一是检测并删除非法代码，二是阻止非法代码对主机系统造成伤害。第一种功能和杀毒软件相似，通过在接收到的信息中检测病毒特征来发现非法代码。由于黑客通常将非法代码分散在多个 TCP 报文中，因此，网络入侵防御系统必须将属于同一 TCP 连接的多个 TCP 报文净荷拼装后，才能检测出包含在信息中的病毒特征，这种处理过程非常费时，会降低网络入侵防御系统的转发速率，因此，由主机入侵防御系统完成非法代码检测是比较合适的。第二种功能要阻止已知和未知的非法代码对主机系统实施的攻击。网络入侵防御系统对未知攻击是很难防御的，但主机入侵防御系统由于可以监管到最终在主机上展开的操作，因此，可以通过判别操作的合理性来确定是否是攻击行

为,如网络下载的某个软件运行时,企图使用属于其他进程的存储器空间,可以确定该软件带有存储器溢出攻击的非法代码,主机入侵防御系统通过终止该软件的运行来阻止非法代码可能对主机系统造成的伤害。如主机入侵防御系统监控到 OUTLOOK 进程企图生成另一个子进程时,可以确定用户运行了邮件附件中的非法代码,可以通过立即终止该子进程来防止非法代码的传播。

2) 有效管制信息传输

主机入侵防御系统一方面可以对主机发起建立或主机响应建立的 TCP 连接的合法性进行监控,另一方面,可以对通过这些 TCP 连接传输的信息进行检测,如果发现通过某个 TCP 连接传输的信息是主机入侵防御系统定义为敏感信息的文件内容,可以确定主机中存在后门或间谍软件,主机入侵防御系统将立即释放该 TCP 连接并记录下该 TCP 连接的发起或响应进程,包含敏感信息的文件的路径、属性和名称等相关信息,以便网络安全管理员追踪、分析可能发生的攻击。

3) 强化对主机资源的保护

主机资源主要有 CPU、内存、连接网络的链路和文件系统等,主机入侵防御系统可以为这些资源建立访问控制阵列,访问控制阵列给出每一个用户和进程允许访问的资源、资源访问属性等,根据访问控制阵列对主机资源的访问过程进行严格控制,以此实现对主机资源的保护。

2. 网络入侵防御系统

1) 保护网络资源

主机入侵防御系统只能保护主机免遭攻击,需要网络入侵防御系统保护结点和链路免遭攻击,如一些拒绝服务攻击就是通过阻塞链路达到使正常用户无法正常访问网络资源的目的。

2) 大规模保护主机

主机入侵防御系统只能保护单台主机免遭攻击,如果一个系统中有成千上万台主机,每一台主机都安装主机入侵防御系统是不现实的,一是成本太高,二是使所有主机入侵防御系统的访问控制策略一致也很困难。而单个网络入侵防御系统可以保护一大批主机免遭攻击,如图 8.1 中的网络入侵防御系统可以有效保护内网中的终端免遭外网黑客的攻击。

3) 和主机入侵防御系统相辅相成

主机入侵防御系统由于能够监管发生在主机上的所有操作,而且可以通过配置列出非法或不合理操作,从而通过最终操作的合理和合法性来判别主机是否遭受攻击,这是主机入侵防御系统能够检测出未知攻击的主要原因。但有些攻击是主机入侵防御系统无法检测的,如黑客进行的主机扫描,主机入侵防御系统无法根据单个被响应或被拒绝的 TCP 连接请求确定黑客正在进行主机或端口扫描,但网络入侵防御系统根据规定时间内由同一主机发出的超量 TCP 连接请求确定网络正在遭受黑客的主机扫描侦察。

8.1.2 入侵防御系统工作过程

1. 网络入侵防御系统工作过程

1）捕获信息

网络入侵防御系统是一种对传输信息进行异常检测的设备，因此，首先必须具有捕获信息的功能，捕获信息是指能够截获需要检测的信息，图 8.2 就是网络入侵防御系统捕获信息的过程。

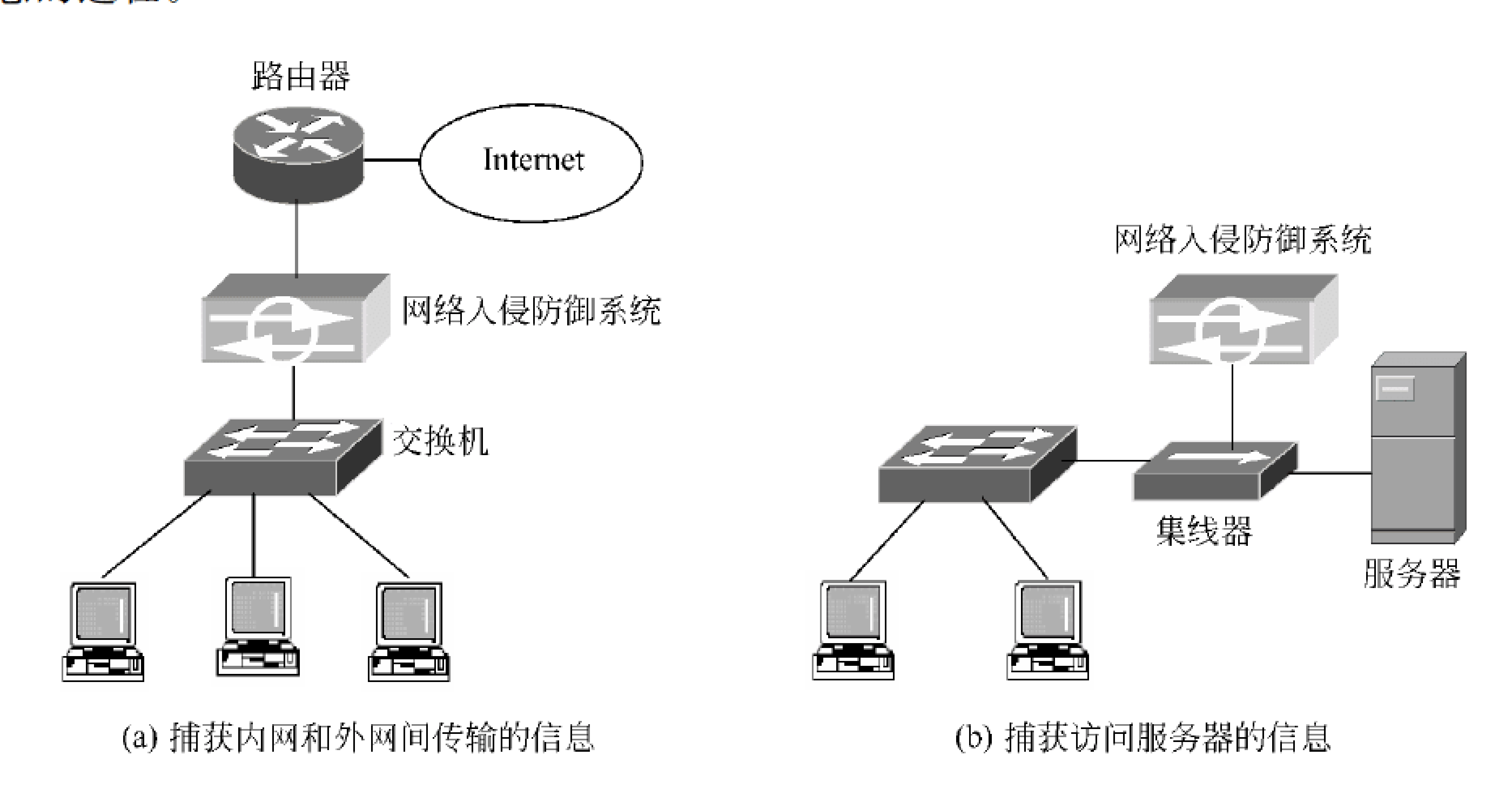


图 8.2 信息捕获过程

图 8.2(a)给出了网络入侵防御系统捕获内网和外网之间传输的信息的过程，这种捕获方式要求内网和外网间传输的信息必须经过入侵防御系统转发，增加了入侵防御系统反制异常信息的能力。图 8.2(b)给出了网络入侵防御系统捕获终端和服务器间传输的信息的过程，这种捕获方式下，终端和服务器间交换的信息不需要经过入侵防御系统转发，因此，入侵防御系统无法过滤掉异常信息。从图 8.2 中可以看出，网络入侵防御系统能够捕获到的信息和网络入侵防御系统在网络中的位置有关，如图 8.2(a)中的网络入侵防御系统就无法捕获内网终端间传输的信息，因此，必须根据网络拓扑结构和信息传输模式精心选择网络入侵防御系统在网络中的位置，这样，才能真正起到监测网络中信息的目的。

2）检测异常信息

一种异常信息是包含非法代码的信息，如一个包含病毒的网页，检测这种异常信息的方法和杀毒软件相似，需要提供病毒特征库，网络入侵防御系统通过检测信息中是否包含病毒特征库中的一种或几种特征来确定信息是否异常。另一种异常信息是信息内容和指定应用不符的信息，如目的端口号为 80，但信息内容并不是 HTTP 报文，或者，虽然是 HTTP 报文，但报文中一些字段的取值和 HTTP 要求不符。检测这种类型的异常信息先通过报文的目的端口字段值确定对应的应用层协议，然后通过分析报文内容是否符合协议规范来确定信息是否异常。第三种异常信息是实施攻击的信息，如指针炸弹，指针炸弹利用了服务器中的指针守护程序转发服务请求的功能，指针守护程序将符号@前面的

服务请求转发给紧接着符号@后面的服务器，如果符号@后面紧接着符号@，意味着再次转发服务请求，这样，如果某个服务请求和服务器之间有着一串连续的符号@，如下列服务请求格式：

```
jdoe@@@@@@@@@@@NETSERVER
```

服务请求将被重复转发给服务器，导致服务器资源耗尽，因此，包含上述服务请求格式的信息就是实施攻击的信息。这种用于鉴别是否是攻击信息的字符串模式，称为攻击特征，它和病毒特征相似。为了鉴别攻击信息，需要建立攻击特征库，库中给出了已知攻击的所有特征，对于一些攻击而言，匹配到单个攻击特征就可确定为攻击信息，这样的攻击特征称为元攻击特征，但对于其他一些攻击，可能需要匹配到分散在信息流中的多个攻击特征才能确定为攻击信息。这样的攻击特征称为有状态攻击特征。

3）反制异常信息

如果监测到异常信息，网络入侵防御系统可以对异常信息采取反制动作。

（1）丢弃 IP 分组。

丢弃 IP 分组分为丢弃单个 IP 分组、丢弃所有和异常信息源 IP 地址相同的 IP 分组、丢弃所有和异常信息目的 IP 地址相同的 IP 分组和丢弃所有源和目的 IP 地址都和异常信息相同的 IP 分组。

如果在单个 IP 分组中检测到元攻击特征，可以选择只丢弃单个包含元攻击特征的 IP 分组，以此防御黑客攻击。这种反制动作的好处是当黑客冒用有效 IP 地址实施攻击时，既有效地防御了攻击，又不对正常拥有该 IP 地址的用户造成伤害。

如果黑客攻击过程是一个包含侦察、攻击目标选择和实施攻击这样一些阶段的漫长过程，应该及时阻断黑客和网络之间的联系，这种情况下，选择在一定时间范围内丢弃全部和异常信息源 IP 地址相同的 IP 分组是切断黑客和网络入侵防御系统所保护资源之间联系的有效手段，但对黑客冒用有效 IP 地址实施攻击的情况，有可能影响了正常拥有该 IP 地址的用户访问入侵防御系统所保护资源的过程。

现在的攻击过程往往是分布式攻击过程，黑客控制多个傀儡终端同时发起对某个目标的攻击，这种情况下，切断单个傀儡终端和所攻击的目标资源之间的联系并不能有效遏制攻击过程，因此，一旦检测到异常信息，选择在一定时间范围内丢弃所有和异常信息目的 IP 地址相同的 IP 分组是切断所有傀儡终端和攻击目标之间的联系的最简单方法，但问题是可能影响了许多正常用户访问网络入侵防御系统所保护的资源的过程。

在检测到异常信息的情况下，选择在一定时间范围内丢弃所有源和目的 IP 地址都和异常信息相同的 IP 分组是一种折中方案，它将有效防御特定黑客对特定资源的攻击。

后三种丢弃 IP 分组的方式显得很粗糙，采用这样的丢弃方式的原因是如果某些资源很重要，一旦有攻击信息到达重要资源所在的服务器并成功实施攻击，后果将不堪设想，而网络入侵防御系统又无法检测出所有已知或未知的攻击，因此，在发现可能存在攻击的情况下，采取极端手段来保障重要资源的安全。这就有点像发现有人企图破坏某个重要军事设施，但又无法百分之百地检查出所有破坏者，为了确保安全，只好封锁该重要军事设施，严禁所有人靠近。

丢弃 IP 分组的反制动作只有图 8.2(a)所示的捕获信息方式才能进行,由于图 8.2(b)所示的捕获信息方式没有转发信息的功能,无法实现丢弃 IP 分组的反制动作。

(2) 释放 TCP 连接。

一旦检测到异常信息,而该异常信息又属于某个 TCP 连接,入侵防御系统通过向该 TCP 连接的发起端或响应端发送 RST 位置 1 的 TCP 控制报文来释放该 TCP 连接,图 8.2 所示的两种信息捕获方式都可实现这种反制动作。

4) 报警

由于网络入侵防御系统无法检测出所有已知或未知的攻击,而且网络入侵防御系统只能对捕获到的信息进行检测,因此,不可能通过网络入侵防御系统解决整个网络的安全问题,但每一段链路的信息流模式都不是独立的,通过对某一段链路的检测,可以分析出整个网络的信息流模式和状态,如一旦某段链路检测出攻击信息,很可能整个网络处于被攻击状态,因此,需要网络安全管理员对整个网络的安全状态进行检测,并对遭受到的攻击进行处理,因此,当网络入侵防御系统检测到攻击信息,不仅需要进行反制动作,还需要向控制中心报警,提醒网络安全管理员应对可能存在的攻击。

5) 登记和分析

网络安全涉及多种网络安全设备,如防火墙和入侵防御系统,这些设备的布置和配置是一个复杂的系统工程,需要根据网络安全状态不时加以调整,这就需要及时了解网络遭受攻击的情况,如黑客位置、攻击类型、攻击目标及攻击造成的损失等,网络入侵防御系统在检测到攻击信息后,需要及时记录下攻击信息的源和目的 IP 地址、源和目的端口号及攻击特征等,并由管理软件对这些信息进行分类、统计和分析,以简单明了的方式为网络安全管理员提供网络安全状态,以便网络安全管理员及时调整网络安全设备的布置和配置。

2. 主机入侵防御系统工作过程

1) 拦截主机资源访问操作请求和网络信息流

非法代码激活、感染和破坏主机资源需要对主机资源进行操作,这种操作最终通过调用操作系统内核的文件系统、内存管理系统、I/O 系统的服务功能得以实现,因此,主机入侵防御系统必须能够拦截所有调用操作系统内核服务功能的操作请求,并对操作请求的合法性进行检测。黑客攻击主机的操作通过网络实现,因此,黑客发送的攻击信息和非法代码以信息流方式进入主机,因此,主机入侵防御系统必须能够拦截所有进入主机的信息流,并加以检测,确定是否包含攻击信息或非法代码。

2) 采集相应数据

为判别调用操作系统内核服务功能的操作请求的合法性,需要获得一些数据,如发出调用请求的应用进程及进程所属的用户、操作类型、操作对象、用户状态、主机位置、主机系统状态等,主机入侵防御系统根据这些数据来确定操作请求的合法性。

3) 确定操作请求或网络信息流的合法性

必须根据正常访问规则和主机系统的安全要求设置访问控制策略,如除用户认可的安装操作外,不允许其他应用进程修改注册表,不允许属于某个用户的应用进程访问其他用户的私有目录等。主机入侵防御系统根据采集到的数据和访问控制策略确定操作是否

合法。

4）反制动作

（1）终止应用进程。

一旦检测到非法操作请求，立即终止发出该非法操作请求的应用进程，并释放为该应用进程分配的所有主机资源。

（2）拒绝操作请求。

操作请求虽然非法，但非法操作请求的操作结果对主机系统的破坏性不大，这种情况下，可以只拒绝该操作请求，但不终止发出该非法操作请求的应用进程。

5）登记和分析

同样，对某台主机的攻击可能也是对网络攻击的一个组成部分，因此，必须将主机遭受攻击的情况报告给网络安全管理员，以便其调整整个网络的安全策略。

8.1.3　入侵防御系统不足

1. 主机入侵防御系统的不足

主机入侵防御系统只是一个应用程序，但它所监管的发生在主机上的操作往往由操作系统实现，因此，一是需要多个和操作系统对应的主机入侵防御系统，二是必须具有拦截用户应用程序和操作系统之间调用、响应过程的能力，这一方面会影响一些应用程序的运行，另一方面也同样存在监管漏洞，而且，由于操作系统无法对主机入侵防御系统提供额外的安全保护，容易发生卸载主机入侵防御系统、修改主机入侵防御系统配置的事件。

2. 网络入侵防御系统的不足

目前大部分网络入侵防御系统是独立设备，因此，除非每一段链路都配置网络入侵防御系统，网络入侵防御系统是无法检测流经网络的所有信息的，这就为黑客入侵提供了可能。

3. 无法有效防御未知攻击

入侵防御系统检测异常信息的机制主要分两类，一类针对已知攻击，另一类针对未知攻击，对于已知攻击，通过分析攻击过程和用于攻击的信息模式，提取出攻击特征，建立攻击特征库，通过对捕获的信息进行攻击特征匹配，来确定是否是攻击信息，只要攻击特征能够真实反映攻击信息不同于其他正常信息的特点，通过建立完整的攻击特征库来检测出已知攻击是可能的。对于未知攻击，首先建立正常操作情况下的一些统计值，如单位时间内访问的文件数、登录用户数、建立的TCP连接数和通过特定链路传输的信息流量等，然后在相同单位时间内实时统计上述参数，并将统计结果和已经建立的统计值比较，如果多个参数出现比较大的偏差，说明网络的信息流模式或主机的资源访问过程出现异常。一是由于建立正常操作情况下的一些统计值时，很难保证主机和网络未受到任何攻击，因此，正常统计值的可靠性并不能保证，二是对于正常的网络资源访问过程，随着用户的不同、用户访问的网络资源的不同，实时统计的参数值的变化很大，因此，很容易将正常的网络资源访问过程误认为是攻击，而真正的攻击却可能因为和建立统计值时的网络操作过程相似而被认为是正常操作。

8.1.4 入侵防御系统发展趋势

1. 融合到操作系统中

主机入侵防御系统应该成为操作系统的一部分，由操作系统对主机资源的访问过程进行监管。用户在访问网络资源前，需要到认证中心申请证书，并在证书中列出对网络资源的访问权限，在以后进行的网络资源访问过程中，都必须在访问请求中携带证书。每当有用户访问主机资源时，操作系统必须核对用户身份和访问权限，只有拥有对该主机资源访问权限的用户，才能进行访问过程，这样，可以有效防止黑客攻击和内部用户的非法访问。

2. 集成到网络转发设备中

独立的网络入侵防御系统无法对流经所有网段的信息进行检测，因此，存在安全漏洞，由于网络中的信息须经交换机、路由器等转发设备转发，因此，将网络入侵防御系统集成到网络转发设备是实现对网络中所有信息进行检测的最佳选择，但由于目前随着链路带宽的提高，转发设备已成为网络性能瓶颈，如果再由转发设备完成需要大量处理时间的入侵检测功能，势必更加影响转发设备的转发性能，因此，需要在转发设备的系统结构上进行改革，尽量采用并行处理方式和模块化结构，但可能增加转发设备的制造成本。

8.2 网络入侵防御系统

8.2.1 系统结构

图 8.3 是网络入侵防御系统的应用方式，探测器是核心设备，负责信息流捕获、分析、异常检测、反制动作执行及报警和登记等操作，探测器通过管理端口和安全管理器相连，为了安全起见，互联探测器和安全管理器的网络与信息传输网络是两个独立的网络，安全管理器负责探测器安全策略的配置，报警信息处理，登记信息分析、归类，最终形成有关网络安全状态的报告提供给网络安全管理员。

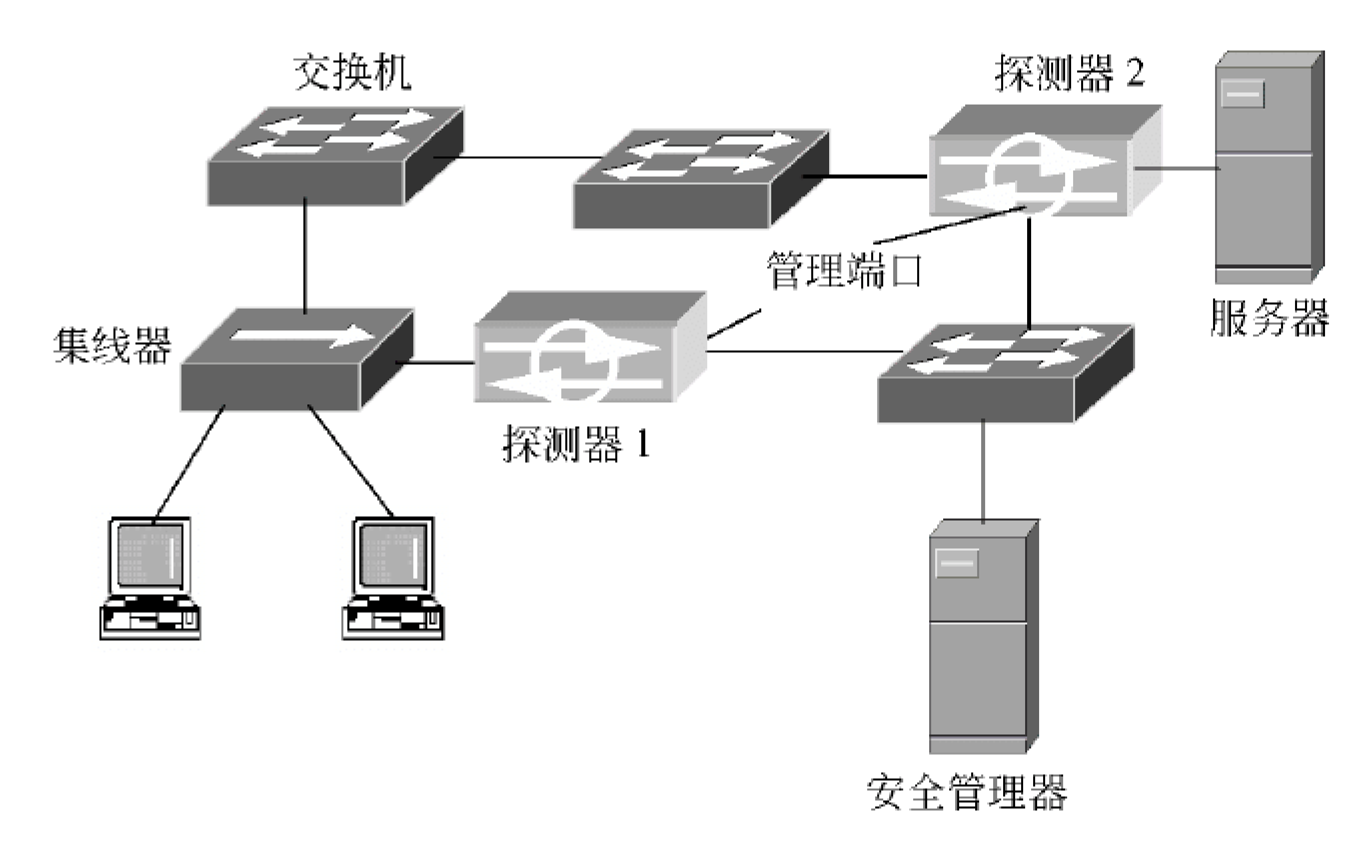


图 8.3 系统结构

探测器可以工作在两种模式：转发和探测，转发模式从一个端口接收信息流，对其进行异常检测，在确定为正常信息流的情况下，从另一个端口转发出去，图 8.3 中的探测器 2 就工作在转发模式。探测模式被动地接收信息流，对其进行处理，发现异常时，向安全管理器报警，并视需要向异常信息流的源和目的终端发送复位 TCP 连接控制报文，图 8.3 中的探测器 1 就工作在探测模式。

8.2.2 信息捕获机制

探测器工作在转发模式时，由于信息流需要经过探测器进行转发，不存在捕获信息流问题，捕获信息流机制主要讨论探测器工作在探测模式时的信息流捕获方法。

1. 集线器

集线器的所有端口构成一个冲突域，从任何一个端口进入的 MAC 帧，将从除接收到 MAC 帧的端口以外的所有其他端口转发出去，因此，连接在集线器上的探测器能够采集到所有经过集线器转发的 MAC 帧，图 8.4 给出了工作在探测模式的探测器捕获终端 *A* 经过集线器发送给终端 *B* 的 MAC 帧的过程。

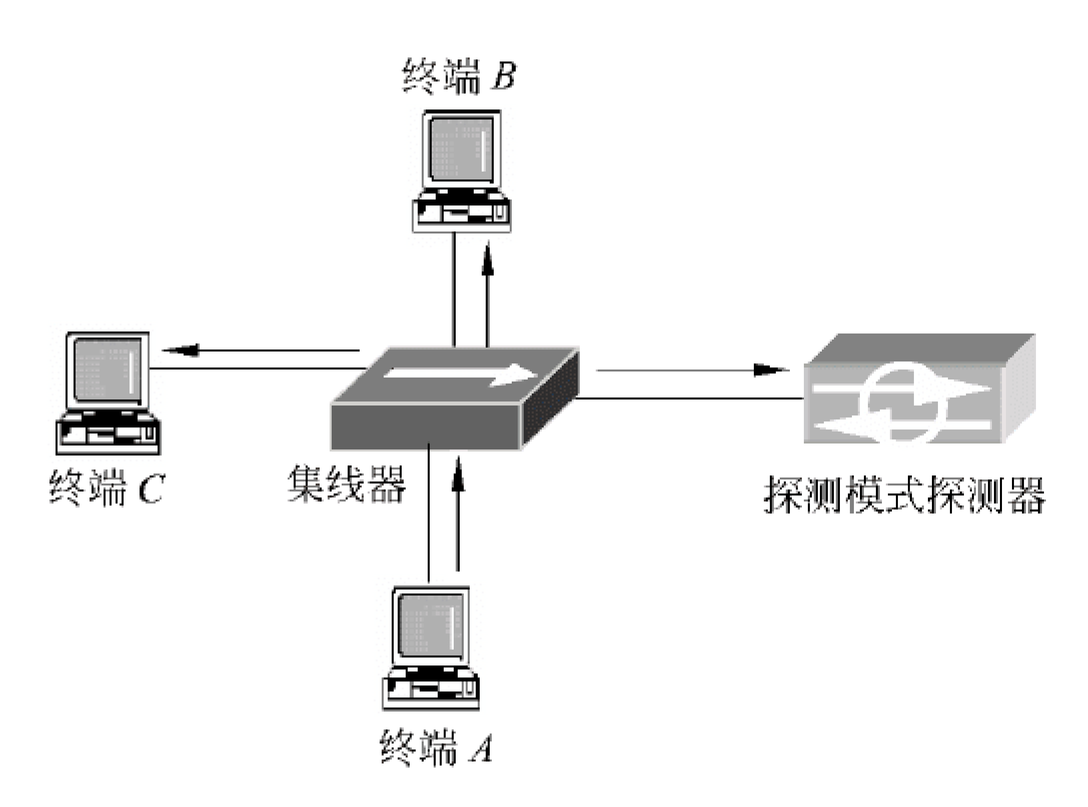


图 8.4　使用集线器捕获信息流机制

2. 交换机端口镜像

交换机和集线器不同，从一个端口接收到 MAC 帧后，用 MAC 帧的目的 MAC 地址检索站表，只从站表中和目的 MAC 地址匹配的端口转发该 MAC 帧，因此，图 8.5 中终端 *A* 发送给终端 *B* 的 MAC 帧，通常只从连接终端 *B* 的端口转发出去，探测器是无法捕获到该 MAC 帧的。但交换机提供了一种称为端口镜像的功能，一旦某个端口配置为另一个端口的镜像，从该端口输出的所有 MAC 帧都被复制到镜像端口，图 8.5 中，如果将交换机端口 2 配置成端口 1 的镜像，则所有从端口 1 发送出去的 MAC 帧都将复制到端口 2，从而被探测器捕获。端口之间的镜像是可以随时改变的，因此，通过将端口 2 配置为不同端口的镜像，探测器可以捕获从不同端口输出的 MAC 帧。

一般交换机支持的端口镜像功能只能实现属于同一个交换机的两个端口之间的镜像功能，这将限制端口镜像功能的信息流捕获能力，为此，有些厂家生产的交换机，如 Cisco 公司的交换机，支持跨交换机端口镜像功能。

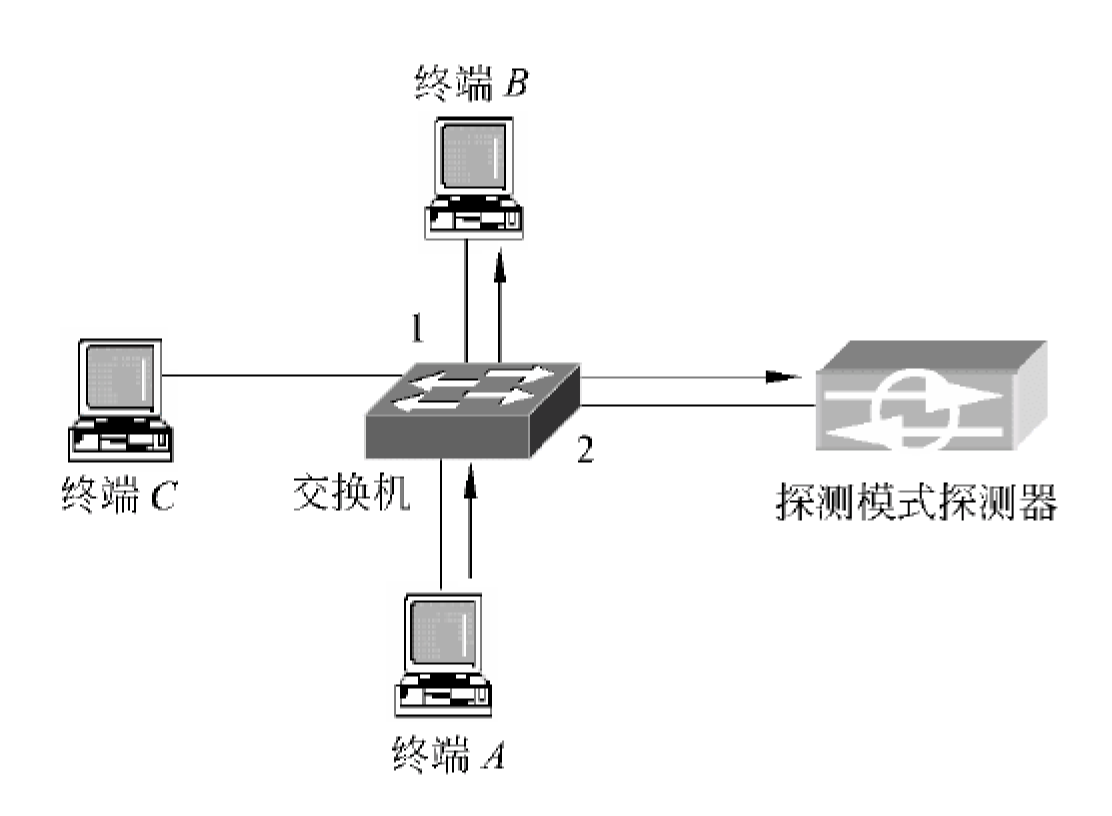


图 8.5 使用交换机端口境像功能捕获信息流机制

如果图 8.6 中探测器需要捕获所有从交换机 1 端口 1 输入的信息流，需要将交换机 1 端口 1、端口 2 和交换机 2 端口 1、端口 2 构成一个特定的 VLAN，所有从交换机 1 端口 1 进入的 MAC 帧，除了正常转发操作外，还需在特定的 VLAN 中广播，这样，终端 *A* 发送给终端 *B* 的 MAC 帧，除了从交换机 1 端口 3 的正常输出外，还需从构成特定 VLAN 的端口中广播出去，最终到达工作在探测模式的探测器。

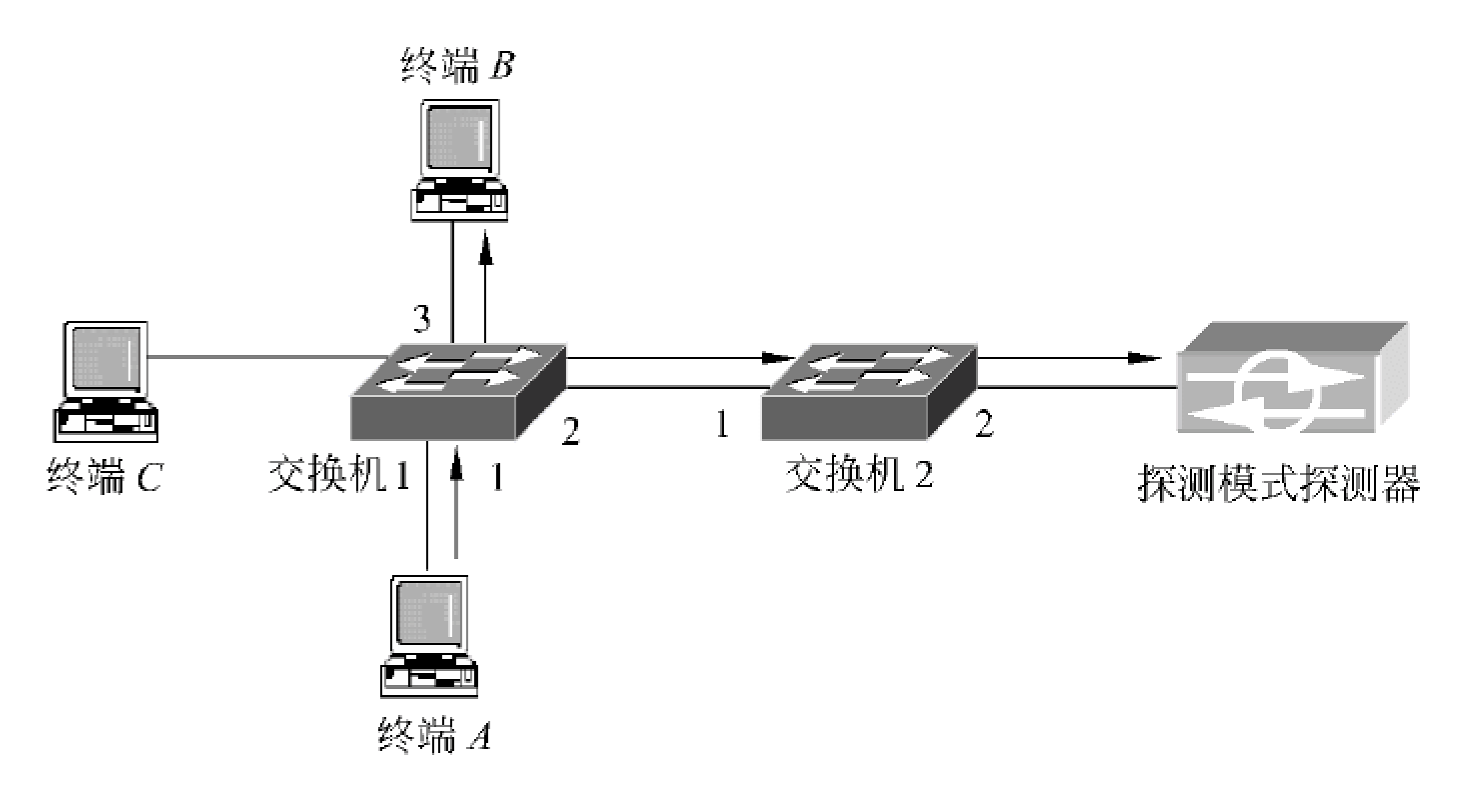


图 8.6 使用跨交换机端口境像功能捕获信息流机制

3. 虚拟访问控制列表

交换机具有策略路由功能，可以为特定的信息流指定传输路径，特定的信息流往往通过源和目的 IP 地址、源和目的端口号等用于标识信息流的属性参数确定。如可以在图 8.7 中的交换机端口 1 设置访问控制项，它由两部分组成，一部分是标识信息流的属性参数组合，另一部分是为符合属性参数组合条件的信息流指定的传输路径，以下就是为端口 1 设置的访问控制项。

- 源 IP 地址：192.1.1.0/24。
- 目的 IP 地址：192.1.2.0/24。
- 协议类型：TCP。
- 源端口号：任意。

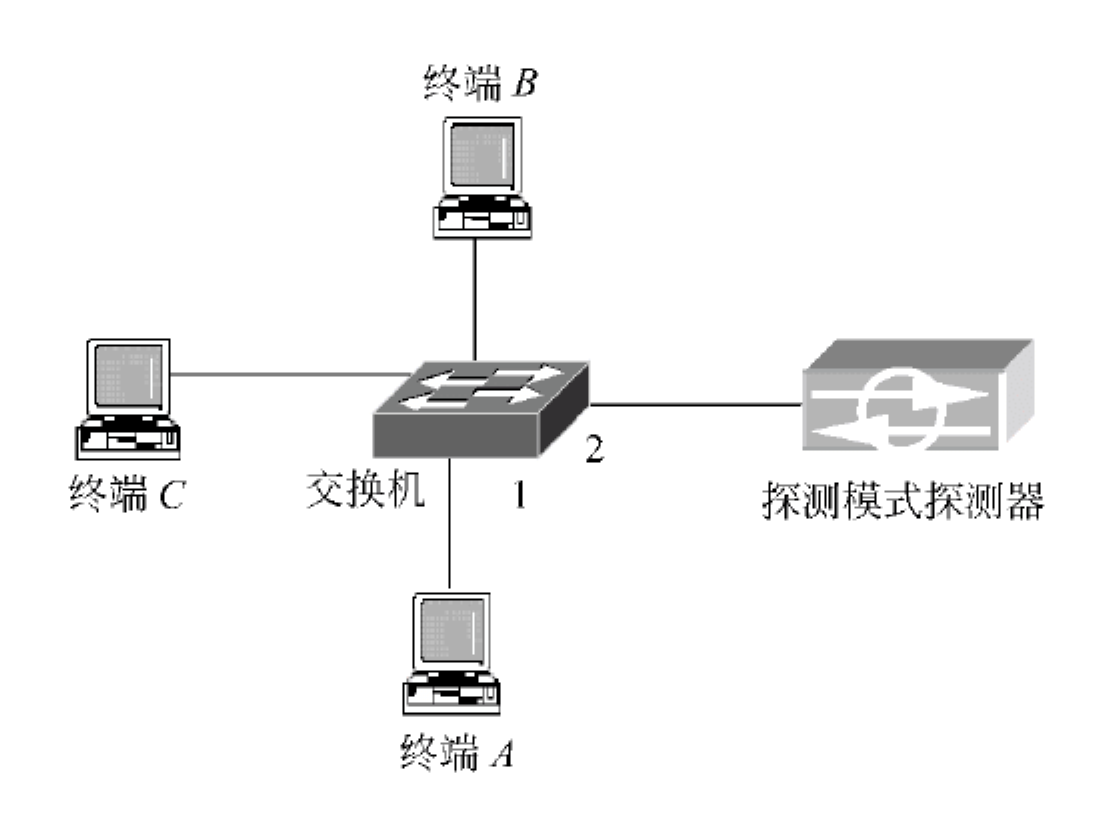


图 8.7　使用虚拟访问控制列表功能捕获信息流机制

• 目的端口号：80。
• 传输路径：端口 2。

一旦在端口 1 中设置了上述访问控制项，所有符合上述属性参数组合条件的信息流都将从端口 2 转发出去。

虚拟访问控制列表中的访问控制项的作用有所改变，符合属性参数组合条件的信息流除了从指定的传输路径转发出去外，还需根据该访问控制项的情况正常进行转发操作，这样，如果为图 8.7 中的交换机端口 1 设置上述虚拟访问控制项，所有经过端口 1 的符合上述组合条件的信息流除了正常转发操作外，还需从端口 2 转发出去，工作在探测模式的探测器因而捕获这些信息流。虚拟访问控制列表可以使探测器捕获特定的信息流，这将为探测器的入侵检测操作带来方便。

8.2.3　入侵检测机制

目前，网络入侵防御系统的入侵检测机制主要可以分为攻击特征检测、协议译码和异常检测三类，攻击特征检测和杀毒软件检测病毒的机制相同，从已经发现的攻击中，提取出能够标识这一攻击的特征信息，构成攻击特征库，然后在捕获到的信息中进行攻击特征匹配操作，如果匹配到某个攻击特征，说明捕获到的信息就是攻击信息。协议译码一是对 IP 分组格式、TCP 报文格式进行检测，二是根据 TCP 报文的目的端口字段值或 IP 报文的协议字段值确定报文净荷对应的应用层协议，然后根据协议要求对净荷格式、净荷中各字段内容及请求和响应过程进行检测，如果发现和协议要求不一致的地方，表明该信息可能是攻击信息。异常检测是建立正常网络访问过程下的信息流模式或正常网络访问规则，然后实时分析捕获到的信息所反映的信息流模式或对网络资源的操作，并将分析结果和已经建立的信息流模式库或操作规则库相比较，如果发现较大偏差，说明发现异常信息。

1. 攻击特征检测

1) 攻击特征分类

攻击特征分为元攻击特征和有状态攻击特征两类，元攻击特征是指用于标识某个攻击的单一字符串，如“/etc/passwd”，只要在捕获到的信息中发现和元攻击特征相同的内

容,如检测到字符串“/etc/passwd”,意味着该信息是攻击信息,元攻击特征检测对每一个IP分组独立进行,与其他IP分组的检测结果无关,但在具体的实现过程中,为了检测出分散在多个TCP报文中的元攻击特征,仍然需要进行TCP报文的拼装操作,如某个TCP报文含有字符串“/etc/passwd”,但攻击者为了躲过网络入侵防御系统的入侵检测,将字符串“/etc/passwd”分散在两个TCP报文中,前一个TCP报文末尾包含字符串“/etc/p”后一个TCP报文开头包含字符串“asswd”,这两个TCP报文封装为两个独立的IP分组,当网络入侵防御系统单独检测这两个IP分组时,都没有找到元攻击特征——字符串“/etc/passwd”。因此,网络入侵防御系统在实施元攻击特征检测时,需要对属于同一TCP连接的TCP报文进行拼装操作,拼装操作通常基于完整的信息行,即拼装后的TCP报文必须包含两组行结束符之间的全部信息,这样,使得网络入侵防御系统可以逐行检测字符串“/etc/passwd”。

有状态攻击特征不是由单一攻击特征标识某个攻击,而是由分散在整个攻击过程中的多个攻击特征标识某个攻击,且这些攻击特征的出现位置和顺序都有着严格的限制。只有在规定位置、按照规定顺序检测到全部攻击特征,才能确定发现攻击。图8.8是有状态攻击特征的示意图,它用事件轴的方式给出攻击过程中每一个阶段的攻击特征,因此,有状态攻击特征首先需要划分阶段,给出每一个阶段的起止标识。或者用某个操作过程,如建立TCP连接过程,作为一个阶段。或者用TCP报文净荷内容的某个段落作为一个阶段,如HTTP报文的开始行和首部行作为一个阶段,HTTP报文的实体作为另一个阶段。然后给出每一个阶段需要匹配的攻击特征。由于不同阶段往往涉及不同的IP分组,只有按照顺序在每一个阶段检测到对应的攻击特征时才能确定发现攻击,因此,需要网络入侵防御系统保存每一个阶段的检测状态,这是称这种检测机制为有状态攻击特征的原因。

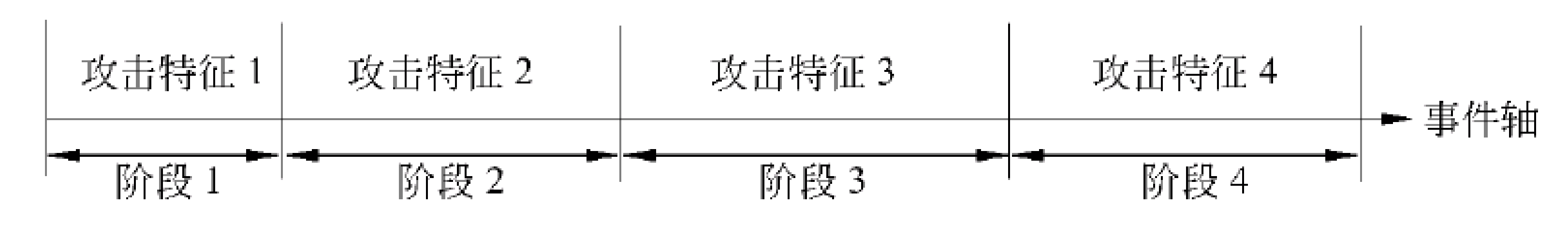


图8.8 描述某个攻击的事件轴

在HTTP URL中检测字符串“/etc/passwd”是有状态攻击特征,它指定三个阶段:TCP连接建立、应用层协议标识和HTTP开始行。TCP连接建立阶段的攻击特征是有效TCP连接,意味着只对经过有效TCP连接传输的信息进行检测;应用层协议标识阶段的攻击特征是服务器端口号必须为80,即TCP连接建立时,响应端的端口号必须是80,表明是用于传输HTTP报文的TCP连接;HTTP开始行的攻击特征是URL中包含字符串“/etc/passwd”。入侵防御系统只有按照顺序在三个阶段同时检测到攻击特征时,即一是检测到成功建立的TCP连接;二是TCP连接响应端的端口号为80;三是在属于该有效TCP连接的TCP报文中,在HTTP开始行URL内容中发现字符串“/etc/passwd”;确定发现攻击。

通常情况下,只要提取出的攻击特征具有唯一标识某个攻击的特性,利用攻击特征检测攻击的准确率是很高的,就像用病毒特征库检测病毒一样。但由于攻击特征库不是保密的,攻击者很可能用大量包含某个攻击特征的信息来触发防御操作,以此影响网络入侵

防御系统的正常操作。

2）攻击特征表示

需要用规范的表示方法表示出：包含在任意位置的字符串“/etc/passwd”，或者 URL 内容中包含字符串“/etc/passwd”，下面是 NETSCREEN 入侵防御设备用于表示攻击特征的方法，语法和说明见表 8.1。

表 8.1　攻击特征表示方法

<table>
<tr><th>语　　法</th><th>说　　明</th></tr>
<tr><td>\0＜八进制数字＞</td><td>直接用八进制数字表示攻击特征</td></tr>
<tr><td>\X＜十六进制数字＞\X</td><td>直接用十六进制数字表示攻击特征</td></tr>
<tr><td>\[＜字符集＞\]</td><td>大小写无关字符集</td></tr>
<tr><td>.</td><td>任意一个字符</td></tr>
<tr><td>*</td><td>0 次或重复多次前面字符</td></tr>
<tr><td>+</td><td>1 次或重复多次前面字符</td></tr>
<tr><td>|</td><td>多项并列</td></tr>
<tr><td>[＜开始字符＞－＜结束字符＞]</td><td>字符范围</td></tr>
</table>

根据表 8.1 给出的攻击特征表示方法，可以给出表 8.2 所示的攻击特征表示实例。

表 8.2　攻击特征表示实例

<table>
<tr><th>表示实例</th><th>含　　义</th><th>匹　配　实　例</th></tr>
<tr><td>\X01 86 A5 00 00\X</td><td>5 个十六进制表示的字节</td><td>01 86 A5 00 00</td></tr>
<tr><td>\[hello\]</td><td>大小写无关字符串</td><td>hElLo
HElIO
heLLO</td></tr>
<tr><td>[c－e]a(d|t)</td><td>c、d 或 e 开头，第 2 个字符为 a，以字符 d 或 t 结束</td><td>cad
cat
dad
dat
ead
eat</td></tr>
<tr><td>a * b+c</td><td>任意个数的字符 a，紧跟 1 个或多个字符 b，最后以字符 c 结束</td><td>bc
abc
aaaabbbbc</td></tr>
<tr><td>. * @@. *</td><td>包含@@的任意字符串</td><td>jdoe@@@@@@@@@@@NETSERVER</td></tr>
<tr><td>. * /etc/passwd. *</td><td>包含/etc/passwd 的任意字符串</td><td>HTTP://WWW.ABC.COM/etc/passwd</td></tr>
<tr><td>(GET | HEAD) . * /etc/passwd. *</td><td>以 GET 或 HEAD 开始，包含/etc/passwd 的字符串</td><td>GET HTTP://WWW.ABC.COM/etc/passwd
HEAD HTTP://WWW.ABC.COM/etc/passwd</td></tr>
</table>

2. 协议译码

协议译码可以在三个层次对捕获的信息进行检测，一是对IP分组格式和各个字段值进行检测；二是对TCP报文格式和各个字段值进行检测；三是根据TCP报文的目的端口字段值或IP报文的协议字段值确定报文净荷对应的应用层协议，然后根据协议要求对净荷格式、净荷中各字段内容及请求和响应过程进行检测。

1）IP分组检测

IP分组检测主要检测IP分组各个字段值是否符合协议要求，重点检测分片是否正确，因为一些攻击是将TCP报文首部分散在多片数据中，以此绕过对TCP首部字段值的检测，因此，单个IP分组的分片必须完整包含整个TCP报文首部。另一种攻击是超大IP分组，即所有分片拼装后的总长度超过64KB，由于每一个IP分组的总长限制在64KB，一些IP接收进程对缓冲器长度的默认限制是64KB，因此，当IP接收进程拼装一个总长大于64KB的IP分组时，可能导致缓冲器溢出，并使系统崩溃。

2）TCP报文检测

建立TCP连接时由双方确定初始发送序号，数据交换过程中接收端通过确认序号和窗口字段值确定发送端的发送窗口，因此，可以通过跟踪双方发送、接收的TCP报文确定任何时刻两端的发送窗口，由此确定经过该TCP连接传输的TCP报文的发送序号范围，因此可以通过检测经过该TCP连接传输的TCP报文的发送序号来确定是否是攻击者盗用该TCP连接传输攻击信息。

TCP进程将应用层数据分段后进行传输，各段数据的序号应该连续且没有重叠，TCP接收进程如果接收到相邻且序号重叠的TCP报文时，可能出错，并使系统崩溃，因此，TCP报文检测的另一个任务是对发送序号在接收端接收窗口内的TCP报文进行虚拟拼装操作，以此发现序号重叠的相邻数据段，并予以丢弃，预防接收端TCP进程因为序号重叠错误而崩溃。

3）应用层协议检测

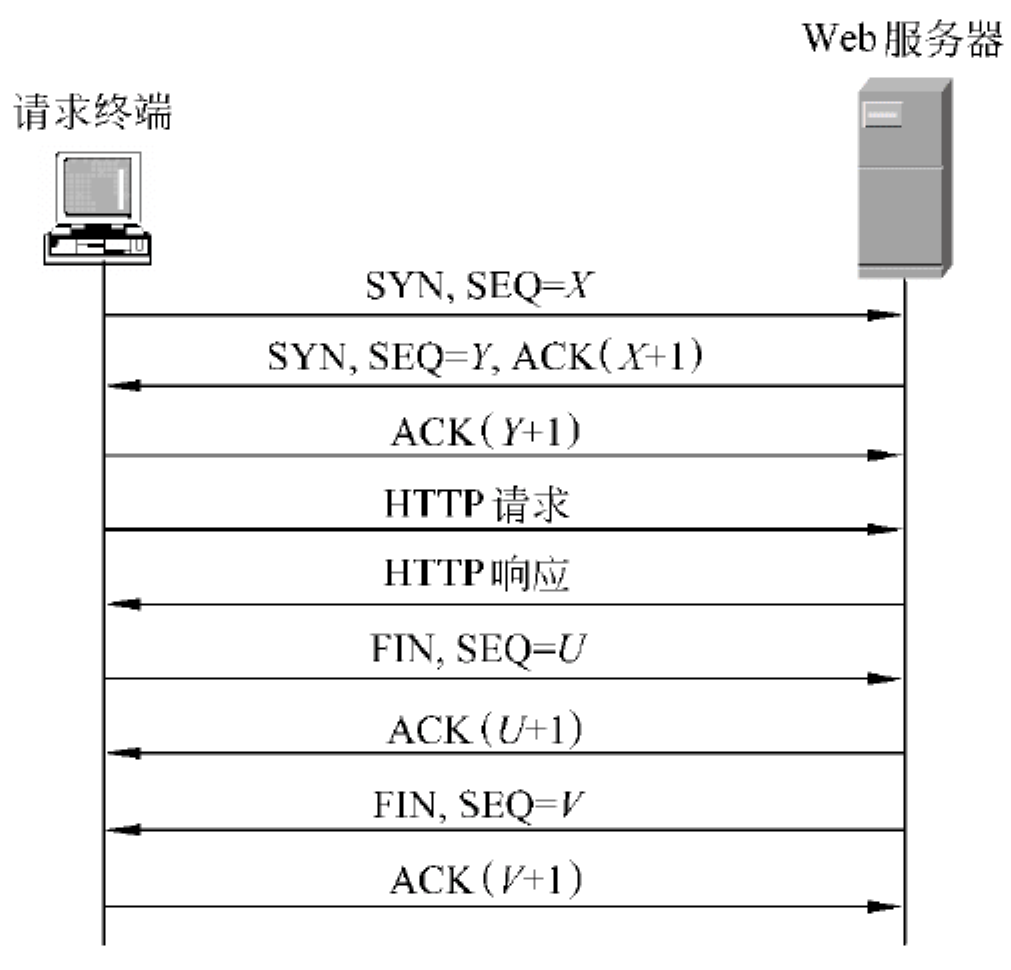
应用层协议检测首先判定TCP报文服务器端端口号字段值和TCP报文净荷内容是否一致，一旦发现不一致，丢弃这些TCP报文。这样做的原因是一些用户知道大部分防火墙会允许访问Web服务器的信息流在内外网之间传输，因此，将实现P2P的TCP连接的服务器端端口号设定为80，以此绕过防火墙的检测。另外，一些黑客也有可能冒用一些常用的著名端口号，如80，来伪装用于传输攻击信息的TCP报文。

应用层检测在确定TCP报文净荷内容和服务器端端口号字段值一致的情况下，根据应用层协议要求检查各个字段值是否在合理范围内，丢弃包含不合理字段值的应用层数据。

应用层检测还需监控应用层协议的操作过程，HTTP的正常操作过程如图8.9所示，应用层协议检测将监测HTTP请求、响应过程是否如图8.9所示，响应内容和请求内容是否一致，一旦发现异常，确定为攻击信息。

3. 异常检测

异常检测的前提是正常访问网络资源的信息流模式或操作模式和入侵者用于攻击网



注：ACK(Y+1)表示确认序号为Y+1

图 8.9 HTTP 正常操作过程

络或非法访问网络资源的信息流模式或操作模式之间存在较大区别。首先需要确定正常访问网络资源的信息流模式或操作模式，然后实时分析捕获到的信息所反映的信息流模式或操作模式，如果通过比较发现后者和前者之间存在较大偏差，确定捕获到的信息异常。因此，实现异常检测的第一步是建立正常访问网络资源的信息流模式和操作模式，目前存在两种用于建立正常访问网络资源的信息流模式和操作模式的机制，它们分别是基于统计机制和基于规则机制。

1）基于统计机制

网络入侵防御系统在确保网络处于正常访问状态下，对捕获到的信息进行登记，对于流经网络入侵防御系统的每一个 IP 分组，主要登记如下内容：源和目的 IP 地址、源和目的端口号、IP 首部协议字段值、TCP 首部控制标志、报文字节数、捕获时间等。

通过分析登记信息，网络入侵防御系统可以生成两类基准信息：一类是阈值，如单位时间内建立的 TCP 连接数，传输的 IP 分组数、字节数，特定终端发送的建立 TCP 连接请求报文数，对特定服务器发起的建立 TCP 连接请求数等。另一类是描述特定终端行为，或特定终端和服务器之间行为的一组参数，如特定终端建立 TCP 连接的平均间隔、平均传输速率、平均传输间隔、持续传输时间分布、特定应用层数据分布、TCP 报文净荷长度分布和特定服务器之间具有交互特性的 TCP 连接比例等。

生成基准信息后，网络入侵防御系统可以通过实时分析捕获到的信息，找出和基准信息之间的偏差，如果偏差超过设定的范围，意味着检测到异常信息。如基准信息表明：IP 地址为 193.1.1.1 的终端每秒发送的建立 TCP 连接请求报文数为 500，如果通过实时分析捕获到的信息，发现 IP 地址为 193.1.1.1 的终端目前每秒发送的建立 TCP 连接请求报文数为 1000，可以断定该终端正在实施主机扫描或端口扫描，必须予以防范。如基准信息表明：IP 地址为 193.1.1.1 的终端的平均传输速率为 3Mb/s，超过 100ms 连续成组传输 IP 分组（成组传输是指相邻 IP 分组的时间间隔小于 5μs 的情况）的概率为 1%，电子邮件所占比例为

10%，如果通过实时分析捕获到的信息得出 IP 地址为 193.1.1.1 的终端连续 30 分钟成组传输 IP 分组，30 分钟内实际传输速率达到 16Mb/s，而且电子邮件所占比例高达 60%，可以断定 IP 地址为 193.1.1.1 的终端已经感染蠕虫病毒，并正在实施攻击。

2）基于规则机制

基于规则机制通过分析正常网络访问状态下登记的信息和用户特点总结出限制特定用户操作的规则，如为了防止感染了木马病毒的服务器被黑客终端控制，禁止位于子网 193.1.1.0/24 的用户和位于子网 12.3.4.0/24 中的服务器建立具有交互特性的 TCP 连接，定义具有交互特性的 TCP 连接的规则如下所示。

- 相邻 TCP 报文的最小间隔：500ms。
- 相邻 TCP 报文的最大间隔：30s。
- TCP 报文包含的最小字节数：20B。
- TCP 报文包含的最大字节数：100B。
- 背靠背 TCP 报文的最小比例：50%。
- TCP 小报文的最小比例：80%。

交互特性是指反复处于这样的一种循环状态，终端向服务器发送一个命令，服务器执行命令后，回送执行结果，因此，终端在发送一个命令后，等待服务器回送执行结果，在接收到服务器回送的执行结果后，再发送下一个命令，如图 8.10 所示。由此可以得出终端发送的 TCP 报文的特性如下：

- 相邻 TCP 报文的间隔不能太小，否则可能是成组传输，也不能太大，否则没有了交互性。
- TCP 报文一般是小报文，只需包含单个命令行。
- 往往采用背靠背传输方式，即发送一个 TCP 报文，接收到响应报文后，再发送下一个 TCP 报文。

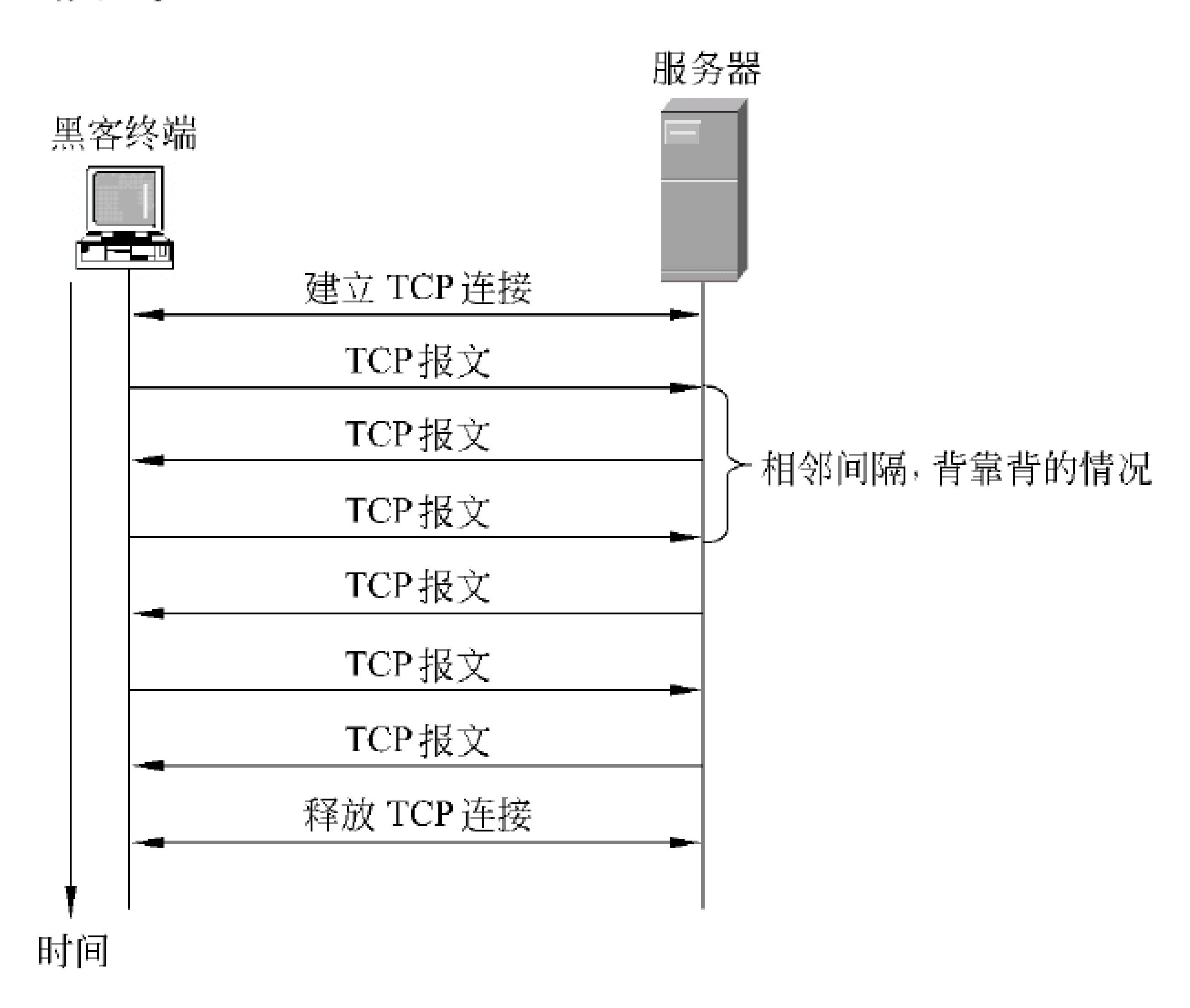


图 8.10 具有交互特性的 TCP 连接

如果网络入侵防御系统定义了上述规则，则在检测到下述情况时确定黑客正通过服务器感染的木马病毒对服务器实施控制如下：

- 成功建立由位于子网 193.1.1.0/24 中的终端发起的，和位于子网 12.3.4.0/24 中服务器之间的 TCP 连接。
- 终端发送的 TCP 报文都是小报文（20B≤包含的数据字节数≤100B）。
- 终端发送的 TCP 报文大部分采用背靠背传输方式（比例超过 70%）。
- 900ms≤终端发送的相邻 TCP 报文之间间隔≤21s。

3）异常检测的误报和漏报

前面已经提到异常检测的前提是正常访问网络资源的信息流模式或操作模式和入侵者用于攻击网络或非法访问网络资源的信息流模式或操作模式之间存在较大区别，但实际上，两者之间虽然存在一定区别，并没有清晰的分界，图 8.11 给出了正常访问过程和攻击过程的行为分布，可以发现，正常访问网络的行为和攻击网络的行为之间存在重叠，这样，对表示异常的阈值设置或行为规则的制定带来一定困难，如果只将 *A* 点左边的行为设定为攻击行为，异常检测的准确性 100%，但将位于 *A* 点和 *B* 点之间原本是攻击过程发生的行为，确认为正常访问过程的行为，存在漏报的问题。同样，如果将 *B* 点左边的行为设定为攻击行为，漏报的问题不复存在，但将位于 *A* 点和 *B* 点之间原本是正常访问过程发生的行为，误认为是攻击过程的行为，产生误报的问题。因此，异常检测虽然能够发现一些未知的攻击，但阈值或行为规则的设定过程比较复杂，需要反复调整，而且，还需根据所保护资源的重要性在误报和漏报之间权衡利弊。

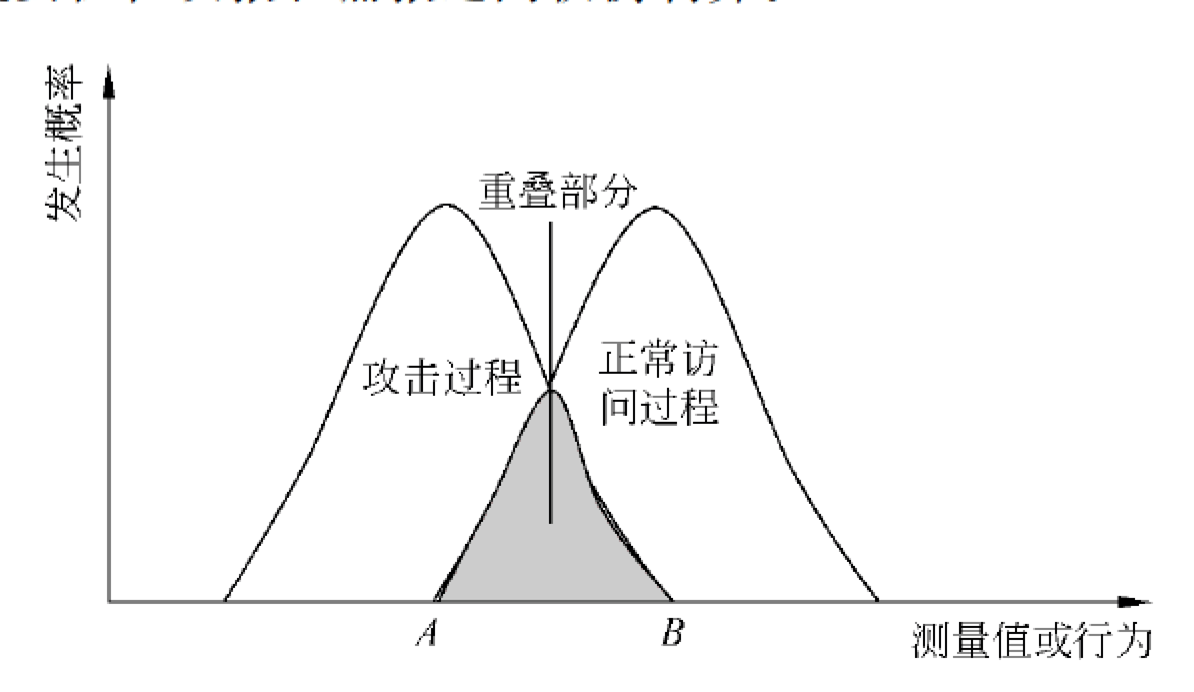


图 8.11　正常访问过程和攻击过程的行为分布

没有一种检测机制可以一劳永逸地解决入侵检测问题，随着攻击过程的步骤越来越多、越来越复杂，黑客攻击的隐蔽性越来越好，简单的检测机制已经很难实现入侵检测，必须研究跟踪能力更强，智能性更高的入侵检测机制。同时，必须具有综合分析多个网段、多种检测机制登记的入侵事件的能力的集中管理器，以此实现对网络的全方位监控。

8.2.4　安全策略

网络结构如图 8.12 所示，网络入侵防御系统用于防御对 Web 和 FTP 服务器的攻击，采用的入侵检测机制包含：攻击特征匹配、协议译码和异常检测。表 8.3 中规则 1 表明只有符合下述全部条件的信息流才能继续转发：

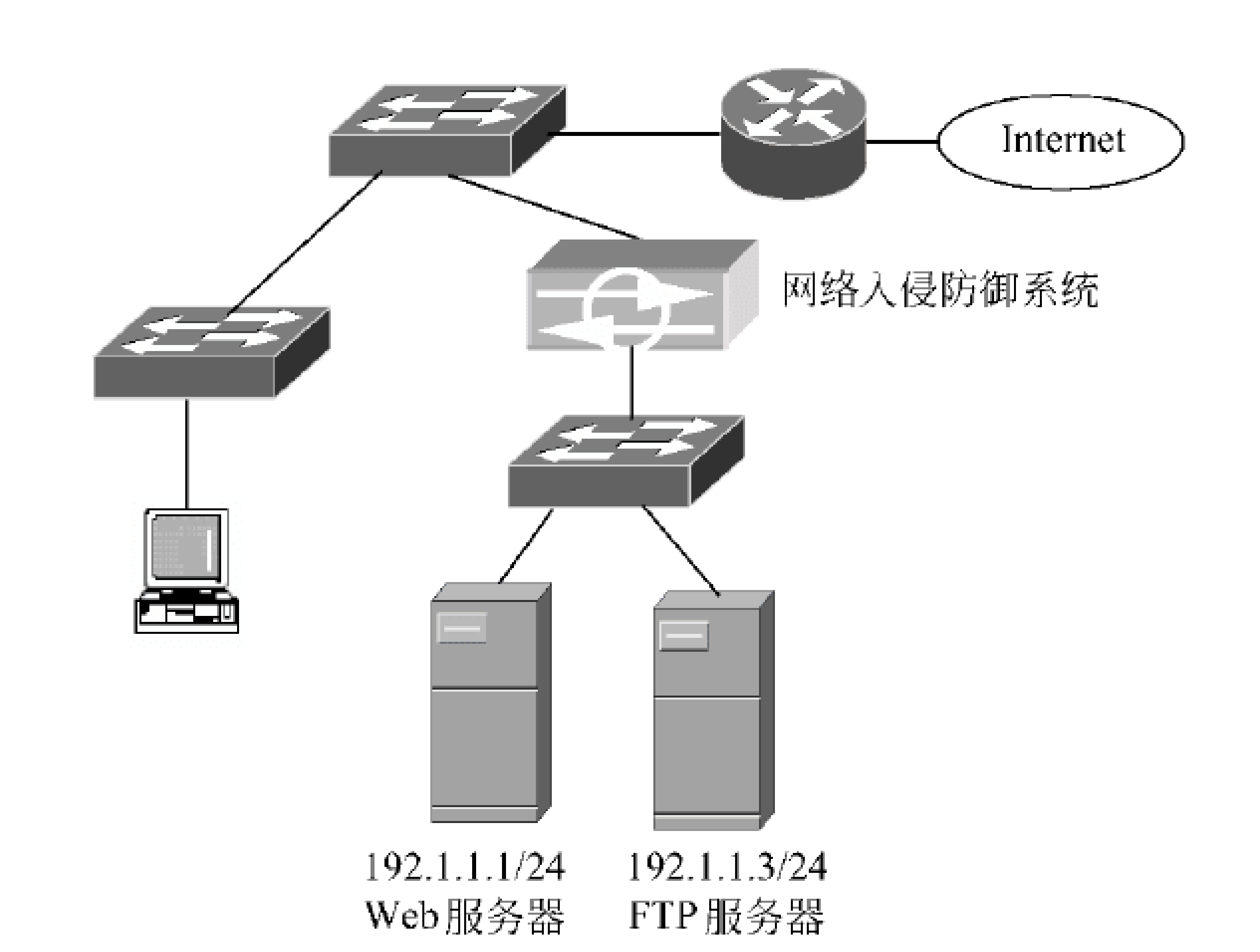


图 8.12 网络结构

表 8.3 安全策略

规则编号	源 IP 地址	目的 IP 地址	服务	攻击特征库/类型	动作
1	任意	192.1.1.1/32	HTTP	HTTP—严重 SYN 泛洪 交互式信息	源 IP 阻塞 丢弃 IP 分组 源 IP 阻塞
2	任意	192.1.1.3/32	FTP	FTP—严重 SYN 泛洪 交互式信息	源 IP 阻塞 丢弃 IP 分组 源 IP 阻塞

- 目的 IP 地址为 192.1.1.1/32；
- IP 首部字段值符合协议规范要求；
- TCP 报文的目的端口号为 80，且应用层数据格式和各字段值符合 HTTP 规范；
- HTTP 报文中不包含攻击特征，用于检测攻击特征的攻击特征库名为 HTTP—严重；
- 单位时间内接收到的用于建立 TCP 连接的请求报文数小于阈值；
- 信息流不具备交互式特性。由于针对不同应用层协议的攻击机制不同，攻击特征也不同，而且，针对同一应用层协议的不同攻击，其危害程度也不相同，因此，常将针对同一应用层协议且危害程度相似的攻击的攻击特征组成一个攻击特征库，如名为 HTTP—严重的攻击特征库中包含针对 HTTP 协议且危害程度严重的攻击的攻击特征。一旦信息流和名为 HTTP—严重的攻击特征库中的某个攻击特征匹配(包含元特征和有状态特征)，探测器将复位传输该信息流的 TCP 连接，并在访问控制列表中添加该信息流的源 IP 地址，执行动作为拒绝传输，当然，可以为这种阻塞操作设置时间范围。根据网络正常情况下统计到的信息流模式设置阈值，如每秒允许建立 500 个 TCP 连接，如果某个单位时间内接收到超过 500 的建立 TCP 连接请求报文，丢弃第 501 个及以后的建立 TCP 连接请求报文。如果在

规定的时间段内，经过某个 TCP 连接传输的信息流具有交互式特性，例如满足如下条件：

- 相邻 TCP 报文的最小间隔＞500ms；
- 相邻 TCP 报文的最大间隔＜30s；
- 背靠背 TCP 报文的比例＞50％；
- TCP 小报文(20B＜TCP 报文包含的字节数＜100B)的比例＞80％。

探测器将复位传输该信息流的 TCP 连接，并在访问控制列表中添加该信息流的源 IP 地址，执行动作为拒绝传输，并为这种阻塞操作设置时间范围。

表 8.3 中规则 2 表明只有符合下述全部条件的信息流才能继续转发：

- 目的 IP 地址为 192.1.1.3/32；
- IP 首部字段值符合协议规范要求；
- TCP 报文的目的端口号为 21，且应用层数据格式和各字段值符合 FTP 规范；
- FTP 控制报文和数据报文中不包含攻击特征，用于检测攻击特征的攻击特征库名为 FTP－严重；
- 单位时间内接收到的用于建立 TCP 连接的请求报文数小于阈值；
- 信息流不具备交互式特性。

8.3　主机入侵防御系统

8.3.1　工作流程

主机入侵防御系统的目的是防止黑客对主机资源的非法访问，因此，必须具有监管发生在主机上的一切操作的能力。图 8.13 给出了主机入侵防御系统的工作流程，首先，它必须能够截获所有对主机资源的操作请求，如调用其他应用进程、读写文件、修改注册表等操作请求，然后，根据操作对象、系统状态、发出操作请求的应用进程和配置的访问控制

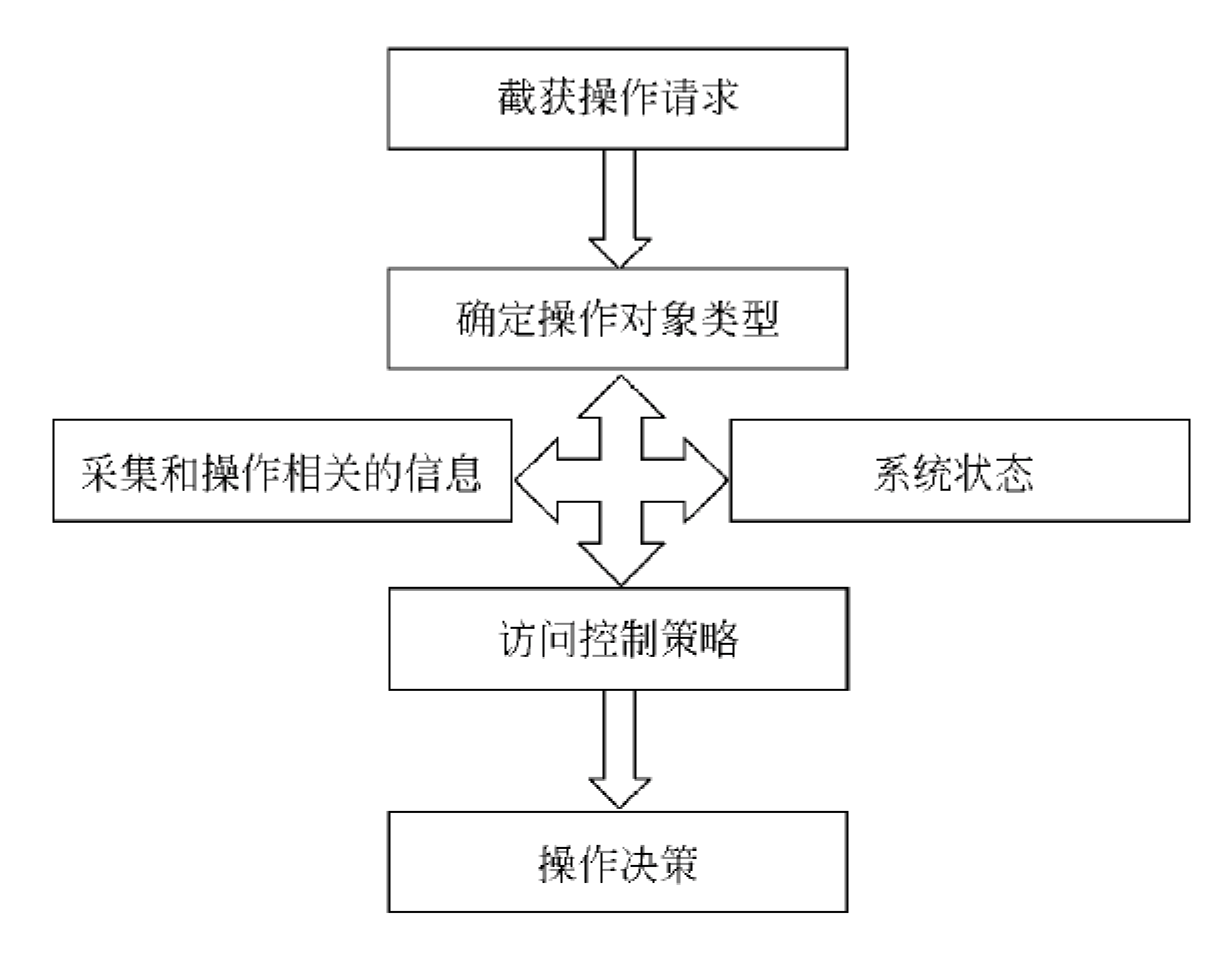


图 8.13　工作流程

策略确定是否允许该操作进行,必要时可能需要由用户确定该操作是否进行,在允许操作继续进行的情况下,完成该操作请求。访问控制策略结合发出操作请求的应用进程和系统状态确定该操作是正常访问,还是恶意攻击,如访问控制策略将 OUTLOOK 调用 CMD. EXE、在非安装程序阶段修改注册表这样的操作请求定义为恶意攻击,予以制止。

8.3.2 截获机制

实现主机入侵防御系统功能的前提是能够截获对主机资源的操作请求,收集和操作相关的参数,这些操作包括对文件系统的访问、对注册表这样的系统资源的访问、TCP 连接建立及其他 I/O 操作等,和该操作相关的参数有操作对象、操作发起者、操作发起者状态等,目前,用于截获操作请求的机制有修改操作系统内核、系统调用拦截和网络信息流监测等。

1. 修改操作系统内核

操作系统的功能一是对主机资源进行管理,二是提供友好的用户接口,对主机资源的操作,如进程调度、内存分配、文件管理、I/O 设备控制等,都由操作系统内核完成,因此,操作系统内核是主机资源操作的最终实施者,由操作系统内核实施入侵防御功能是最直接、最彻底的主机资源保护机制。这种机制下,当操作系统内核接收到操作请求时,先根据操作请求中携带的信息和配置的如表 8.4 所示的访问控制阵列确定是否是正常访问操作,操作系统内核只实施正常访问操作,表 8.4 中给出的是指定用户所启动的某个进程允许访问的主机资源。

表 8.4 访问控制阵列

主机资源	用户	进程	主机资源	用户	进程
资源 *A*	用户 *A*	进程 *A*	资源 *B*	用户 *A*	进程 *A*
资源 *A*	用户 *A*	进程 *B*	⋮	⋮	⋮
资源 *A*	用户 *B*	进程 *A*			

如果由操作系统厂家完成对操作系统内核的修改,主机入侵防御系统就成为操作系统的有机组成部分,这是主机入侵防御系统的发展趋势,但如果由其他方完成操作系统内核的修改,有可能影响第三方软件的兼容性。

2. 系统调用拦截

图 8.14 给出系统调用拦截过程,由于通常由操作系统内核实现对主机资源的操作,因此,应用程序通过系统调用请求操作系统内核完成对主机资源的操作,系统调用拦截程序能够拦截应用程序发出的系统调用,并根据发出系统调用的应用程序、需要访问的主机资源、访问操作类型等数据和配置的访问控制策略确定是否允许该访问操作进行,将允许操作进行的系统调用发送给操作系统内核。由于系统调用拦截程序很容易被屏蔽,因此,采用这种拦截机制的主机入侵防御系统有可能因被黑客绕过,而不起作用,但由于实施比较容易,是目前比较常用的拦截机制。

3. 网络信息流监测

网络信息流在主机内部的传输过程如图 8.15 所示,来自 Internet 的网络信息流被网

卡驱动程序接收后首先传输给属于操作系统内核一部分的TCP/IP组件（Windows的称呼），经过TCP/IP组件处理后，传输给信息流的接收进程，如浏览器或Web服务器（IIS/Apache）。一些攻击的对象并不是网络应用程序，而是TCP/IP组件，对于这种攻击，系统调用拦截程序并不能监测到，必须在网卡驱动程序和TCP/IP组件之间设置监测程序，这就是网络信息流监测器，由它对传输给TCP/IP组件的信息流进行监测，确定信息流的发起者、信息流中是否包含已知攻击特征、拼装后的IP分组的长度是否超过64KB、TCP报文段的序号是否重叠等。

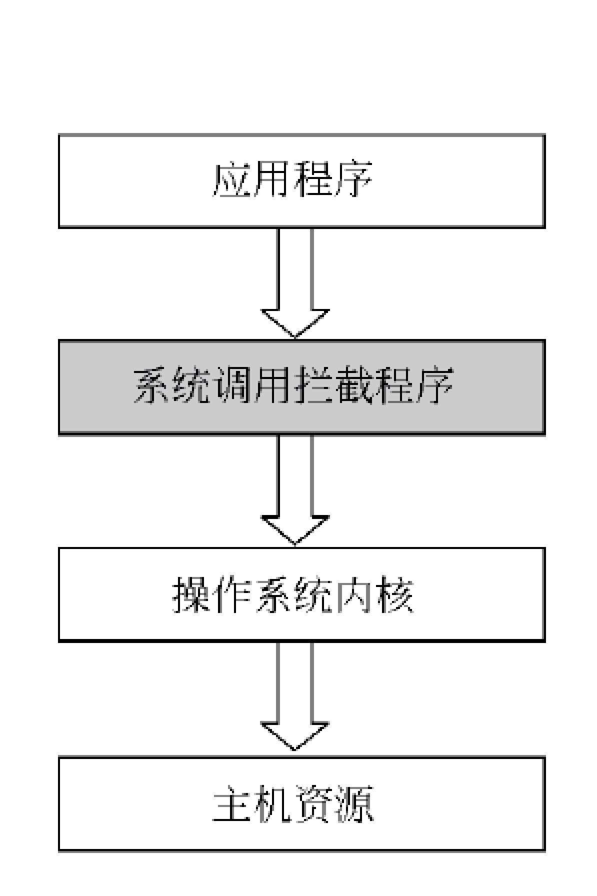


图8.14　系统调用拦截过程

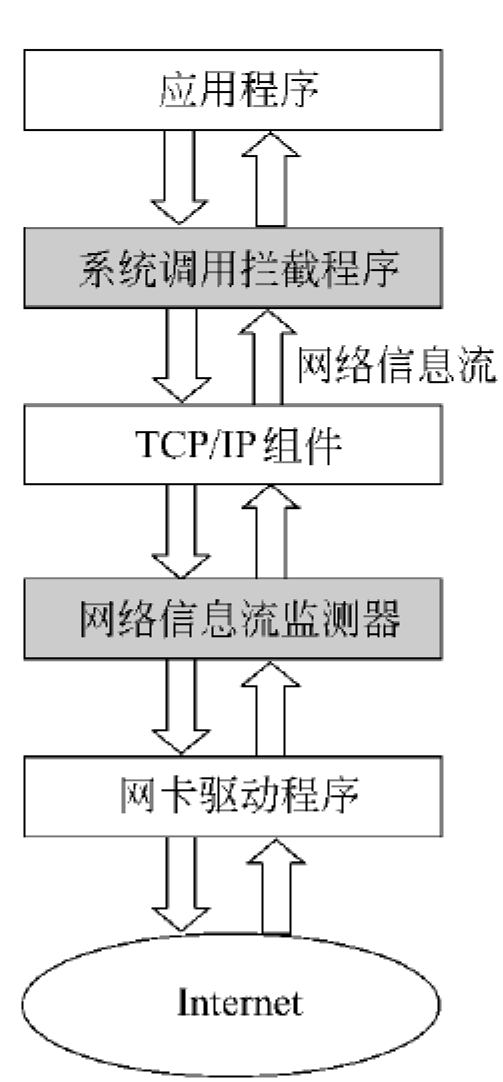


图8.15　网络信息流监测过程

8.3.3　主机资源

主机资源是攻击目标，也是主机防御系统的保护对象，它主要包含网络、内存、进程、文件和系统配置信息。

1. 网络

网络资源是指主机连接网络的通道，通常指TCP连接，当然也包含其他用于实现和Internet进行数据交换的连接方式，如VPN等，黑客发起攻击的第一步是建立黑客终端和被攻击主机之间的传输路径，因此，首先需要占用主机的网络资源，对网络资源的保护是防止黑客攻击的关键步骤，必须对网络资源的使用者、使用过程进行严格控制。

2. 内存

非法代码必须被激活才能实施攻击，激活非法代码意味着需要为非法代码分配内存空间，并将非法代码加载到内存，缓冲器溢出是非法代码加载到内存并被执行的主要手段，因此，必须对分配给每一个进程的内存空间进行严格监管，杜绝任何非法使用分配给某个进程的存储空间的情况发生。

3. 进程

非法代码一旦激活，或者它单独成为一个进程，或者嵌入在某个合法的进程中，因此，

进程是非法代码最终实施感染和攻击的形式，由于进程不是自动产生的，而是由其他进程生成的，必须对生成子进程的过程进行严格监管，防止激活非法代码。

4. 文件

非法代码如果需要长期在某个主机中存在，或者单独作为一个文件或者嵌入在某个文件中，非法代码最终感染或破坏主机的方式也是修改或删除主机中的文件，因此，必须对主机中文件的操作过程实施严格监管，如每个用户只能访问自己的私有文件夹，不允许访问别的用户的私有文件夹，生成或修改可执行文件必须在用户监督下进行。

5. 系统配置信息

系统配置信息通常以系统配置文件形式存在，如 Windows 的注册表、开机后自动启动的程序列表及防火墙配置等，非法代码成功入侵某个主机的前提是成功修改了相关配置信息，使其能够被激活，且具有修改其他文件和其他主机建立 TCP 连接的权限。因此，必须严格管制系统配置信息，尤其是和安全相关的系统配置信息的修改过程。

8.3.4 用户和系统状态

1. 主机位置信息

主机位置和主机对主机入侵防御系统的安全要求有关，如主机位于受防火墙和网络入侵防御系统保护的内部网络时，大量的安全功能由防火墙和网络入侵防御系统完成，主机入侵防御系统实现的访问控制功能要简单一些。当主机位于家庭时，由于缺乏防火墙和网络入侵防御系统的保护，必须由主机入侵防御系统实现所有的访问控制功能。用于确定主机位置的信息有：

- IP 地址；
- 域名前缀；
- VPN 客户信息；
- 网络接口类型(无线网卡还是有线网卡)；
- 其他用于管理该主机的服务器的 IP 地址。

2. 用户状态信息

对于多用户操作系统，可以设置多组具有不同主机资源访问权限的用户，同时为每一个用户设置账号、用户名和口令，当某个用户用对应的用户名和口令登录时，具有了相应的访问权限，因此，主机入侵防御系统对不同用户的主机资源访问控制过程是不一样的，必须为不同类型的用户设置相应的访问控制策略。

3. 系统状态信息

系统状态是指主机系统状态，它同样直接影响着主机入侵防御系统的安全功能，常用的系统状态有：

- 为主机系统设置的安全等级，可以为主机系统设置低、中、高三级安全等级，不同安全等级对应不同的访问控制策略；
- 防火墙功能设置，防火墙设置的安全功能越强，系统的安全性越好，对主机入侵防御系统的依赖越小；
- 主机系统是否遭受攻击，如果监测到端口扫描这样的攻击前侦察行为，主机入侵防御系统的安全功能必须加强；

• 主机工作状态,如在用户允许的程序安装阶段,访问控制策略对配置信息和文件系统的访问控制应该做相应调整;
• 操作系统状态,如检测到漏洞,则必须有针对性地加强主机入侵防御系统的安全功能。

8.3.5 访问控制策略

访问控制策略根据操作请求的发起者、操作类型、操作对象及用户和系统状态确定操作是否进行,通常情况下,先制定不同安全等级的安全策略,然后,将安全策略和用户系统状态绑定在一起构成访问控制策略。安全策略确定操作规则,它通常由以下几部分组成:

• 名字,用于唯一标识该安全策略;
• 类型,用于指明该安全策略用于保护的资源类型,如文件访问控制、注册表访问控制等;
• 动作,操作过程符合规则时触发的动作,如拒绝、登记等;
• 操作请求发起者,用于指明发起操作请求的应用进程类别,如 Web 浏览器,在 Windows 中,该应用进程类别包含 iexplore. exe、netscape. exe、opera. exe、mozilla. exe 等可执行程序;
• 操作,操作请求对操作对象的访问操作,如对某个文件的读写;
• 对象,操作请求的操作对象,如某个文件或注册表等。

表 8.5 给出了一些安全策略实例,其中安全策略 A5、A6 分别允许、拒绝 SSH、Telnet、NFS 进程响应建立 TCP 连接请求。

表 8.5　安全策略实例

名字	类型	动作	操作请求发起者	操作	对象
A1	文件访问控制	拒绝	Web Servers (inetinfo. exe, apache. exe)	写	HTML 文件 (*. html)
A2	注册表访问控制	允许	安装程序(setup.exe,install. exe)	写	Windows run keys (HKLM\software\microsoft\windows\currentversi on\run,runonce,runonceex)
A3	网络访问控制	登记	Web Browsers (iexplore. exe, mozilla. exe,netscape. exe, firefox. exe)	请求建立 TCP 连接	HTTP (TCP/80,TCP/ 443)
A4	应用进程控制	拒绝	所有可执行程序(*. exe)	调用	Command shells (cmd. exe, bash, csh,command. exe)
A5	网络访问控制	允许	SSH Telnet NFS	响应 TCP 连接请求	TCP/22 TCP/23 TCP/2049
A6	网络访问控制	拒绝	SSH Telnet NFS	响应 TCP 连接请求	TCP/22 TCP/23 TCP/2049

表 8.6 结合系统状态给出访问控制策略，表明允许位于内部网络且未遭受攻击的主机开启 SSH、Telnet、NFS 的端口侦听功能，关闭位于家庭且检测到遭受端口扫描侦察的主机的 SSH、Telnet、NFS 的端口侦听功能。

表 8.6 访问控制策略

位置信息	系统状态	安全策略
192.1.1.0/24(单位内部网络)	未遭受攻击	A5
非 192.1.1.0/24(家庭)	端口扫描	A6

8.3.6 Honeypot

Honeypot 是一个虚拟系统，可以是伪装成有丰富资源的 Web 或文件服务器，用于吸引黑客的攻击，Honeypot 上安装功能强大的监测系统，但监测系统不会阻止攻击行为，只是监测整个攻击过程，因此，任何攻击都可在 Honeypot 上成功实现，监测系统将详细记录下整个攻击过程，包含侦察、渗透、驻机、感染和发作。

- 侦察过程：监测系统记录下黑客采用的侦察手段，如端口扫描、登录口令试探等。
- 渗透过程：监测系统记录下黑客采用的渗透手段，如利用操作系统漏洞、邮件附件、后门程序、其他已被攻陷的主机系统等。
- 驻机过程：监测系统记录下黑客采用的将攻击程序常驻在主机中的过程，如添加新文件、修改已有文件、修改注册表等系统配置、安装新的服务、安装后门程序等。
- 感染过程：监测系统记录下黑客采用的扩散攻击程序的过程，如发送附件含有攻击程序的邮件、感染共享文件、通过终端建立的用于访问 Web 服务器或 FTP 服务器的 TCP 连接。
- 发作过程：监测系统记录下攻击程序发作时，对系统进行的破坏操作，如删除或修改文件、降低系统安全等级和防火墙配置的安全功能、盗用系统机密信息、使系统崩溃或拒绝正常服务等。

除此之外，监测系统还将存储下完成整个攻击过程的完整信息流，网络安全管理员通过对监测系统记录下的信息进行分析，找出攻击源、攻击特征和系统安全漏洞，改进网络和主机系统的安全机制。

习 题

8.1 入侵防御系统和有状态分组过滤器的主要功能差异是什么？

8.2 为什么讨论防火墙时重点讨论网络防火墙，而讨论入侵防御系统时，主机入侵防御系统可以和网络入侵防御系统平分秋色？

8.3 网络入侵防御系统和主机入侵防御系统的主要功能差异是什么？

8.4 何为异常信息流？检测异常信息流的机制有哪些？

8.5 网络入侵防御系统中的探测器分为转发模式和探测模式，这两种模式各有什么

优缺点？

8.6　工作在探测模式的探测器如何捕获信息？

8.7　元特征和有状态特征有什么区别？

8.8　入侵防御系统为什么存在误报和漏报攻击的情况？

8.9　攻击特征检测如何解决 TCP 报文分段将攻击特征分散到两个相邻的 TCP 报文中的情况？

8.10　主机入侵防御系统如何监管对主机资源的访问过程？

8.11　主机入侵防御系统如何发现终端感染蠕虫病毒，正在实施病毒传播操作？

8.12　假定网络结构如图 8.16 所示，要求：

- 能够检测感染蠕虫病毒的终端通过发送大量邮件传播病毒的过程；
- 能够检测对服务器发起的猜测登录口令攻击；
- 能够检测黑客终端利用服务器木马病毒控制服务器的操作过程。

给出入侵防御系统设置和配置信息，并简述实现上述要求机制。

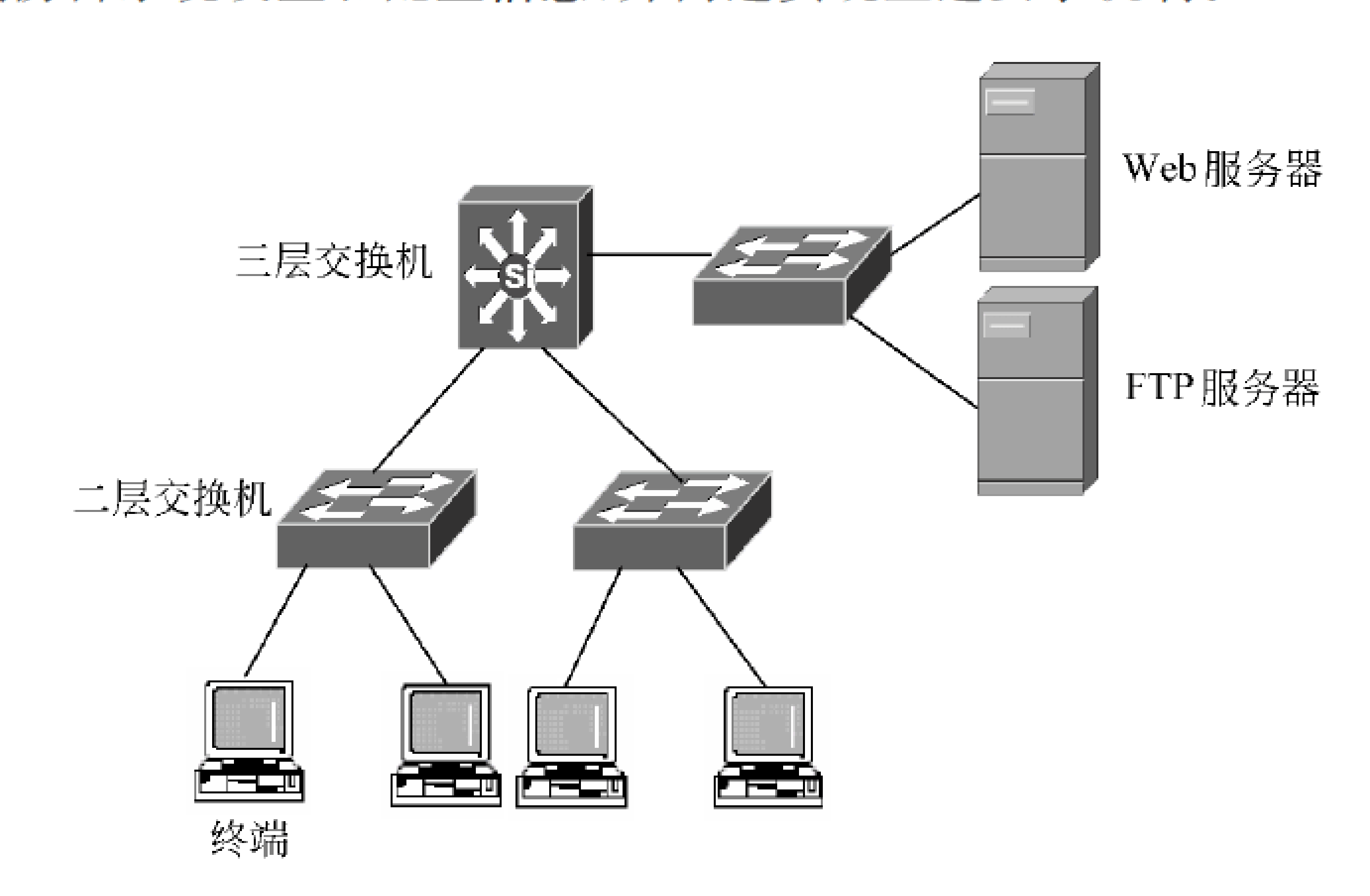


图 8.16　题 8.12 图

8.13　如果图 8.16 中的 FTP 服务器中内容及其敏感，需要严格限制授权终端读取 FTP 服务器中文件的操作，绝不允许删除、修改 FTP 服务器中文件的事情发生，如何通过设置、配置入侵防御系统尽量做到这一点？

第 9 章 CHAPTER

网络管理和监测

9.1 SNMP 和网络管理

随着网络规模的扩大，接入主机的增多和复杂网络应用的开展，网络管理的重要性日益显现，网络管理功能主要包括故障管理、计费管理、配置管理、性能管理和安全管理。故障管理主要包括故障检测、故障隔离和故障修复这三个方面。计费管理用于记录网络资源使用情况，并根据用户使用网络资源的情况计算出需要付出的费用。配置管理包括两方面，一是统一对网络设备参数进行配置；二是为了使网络性能达到最优，采集、存储配置时需要参考的数据。性能管理是指用户通过对系统运行及通信效率等系统性能进行评价，对网络运行状态进行监测，发现性能瓶颈，经过重新对网络设备进行配置，使网络维持服务所需要的性能的过程。安全管理保证数据的私有性，通过用户认证、接入控制等手段控制用户对网络资源的访问，另外，安全管理还包括密钥分配，密钥、安全日志检查、维护等功能。

9.1.1 网络管理系统结构

对于目前这样大规模的网络，用人工监测的方法实施网络管理是不现实的，必须采用自动和分布式管理机制，自动意味着不需要人工监测就能完成网络管理功能，分布式意味着将网络管理功能分散到多个部件中，目前常将网络管理功能分散到网络管理工作站（Network Management Station，NMS）和路由器、交换机、主机等网络结点中，图 9.1 给出常见的网络管理系统结构。

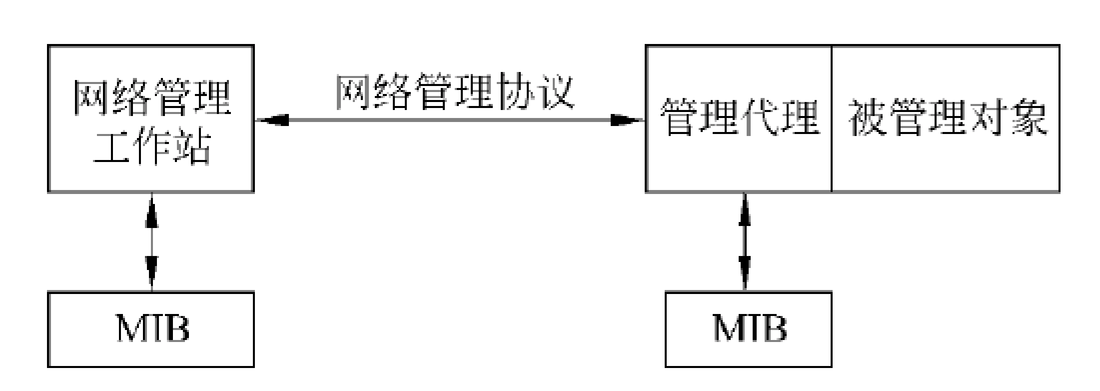


图 9.1 网络管理系统结构

如图 9.1 所示的网络管理系统结构由网络管理工作站、管理代理、管理信息库(Management Information Base,MIB)、被管理对象和网络管理协议组成。

网络管理工作站是一台运行多个网络管理应用程序的主机系统,至少具有以下功能:

- 网络管理员和网络管理系统之间的接口,网络管理员通过网络管理工作站实现对网络系统的监测和控制;
- 运行一系列和网络管理功能相关的应用程序,如数据分析、故障恢复、设备配置、计费管理等;
- 将网络管理员的要求转换成对网络结点的实际监测和控制操作;
- 从网络结点的管理信息库(MIB)中提取出相应信息,构成综合管理数据库,并以用户方便阅读、理解的界面提供整个网络系统的配置、运行状态及流量分布情况。

显然,网络管理工作站实现上述功能的前提是可以和网络结点进行数据交换,能够从网络结点中的管理信息库中获取相关信息,同时,可以向网络结点传输控制命令。

管理代理寄生在路由器、交换机、智能集线器、终端等网络结点中,它一方面负责这些设备的配置,运行时性能参数的采集及一些流量的统计,并将采集和统计结果存储在 MIB 中,另一方面实现和网络管理工作站之间的数据交换,接收网络管理工作站的查询和配置命令,完成信息查询和设备配置操作,对于查询命令,从 MIB 中检索出相应信息,并通过网络管理协议传输给网络管理工作站,对于配置命令,按照命令要求,完成设备中某个被管理对象的配置操作。另外,当管理代理监测到某个被管理对象发生某个重大事件时,也可以通过陷阱,主动向网络管理工作站报告,以便网络管理工作站及时向网络管理员示警,督促网络管理员对网络系统进行干预。

网络管理的基本单位是被管理对象,一个网络结点可以分解为多个被管理对象,每一个被管理对象都有一组属性参数,所有被管理对象的属性参数集合就是管理信息库(MIB),被管理对象是标准的,不同厂家生产的交换机由相同的一组被管理对象进行描述,网络管理工作站通过管理代理对管理信息库中和某个被管理对象相关的属性参数进行操作,如检索和配置,以此实现对该被管理对象的监测和控制。

网络管理协议实现网络管理工作站和网络结点中管理代理之间的通信过程,目前常见的网络管理协议是基于 TCP/IP 协议栈的简单网络管理协议(Simple Network Management Protocol,SNMP),网络管理工作站通过 SNMP,对网络系统进行集中监测和配置。

9.1.2 SNMPv1 基本功能

SNMP 作用过程如图 9.2 所示,网络管理工作站和管理代理之间交换 SNMP 消息,并执行 SNMP 消息包含的命令,SNMP 的命令主要有:

- GET　检索指定被管理对象相关的属性参数值;
- GET NEXT　检索被管理对象树中下一个被管理对象相关的属性参数值,由于被管理对象按照树结构排列,在指定某个被管理对象后,可用 GET NEXT 检索该被管理对象后面的全部被管理对象;
- SET　配置指定被管理对象相关的属性参数;

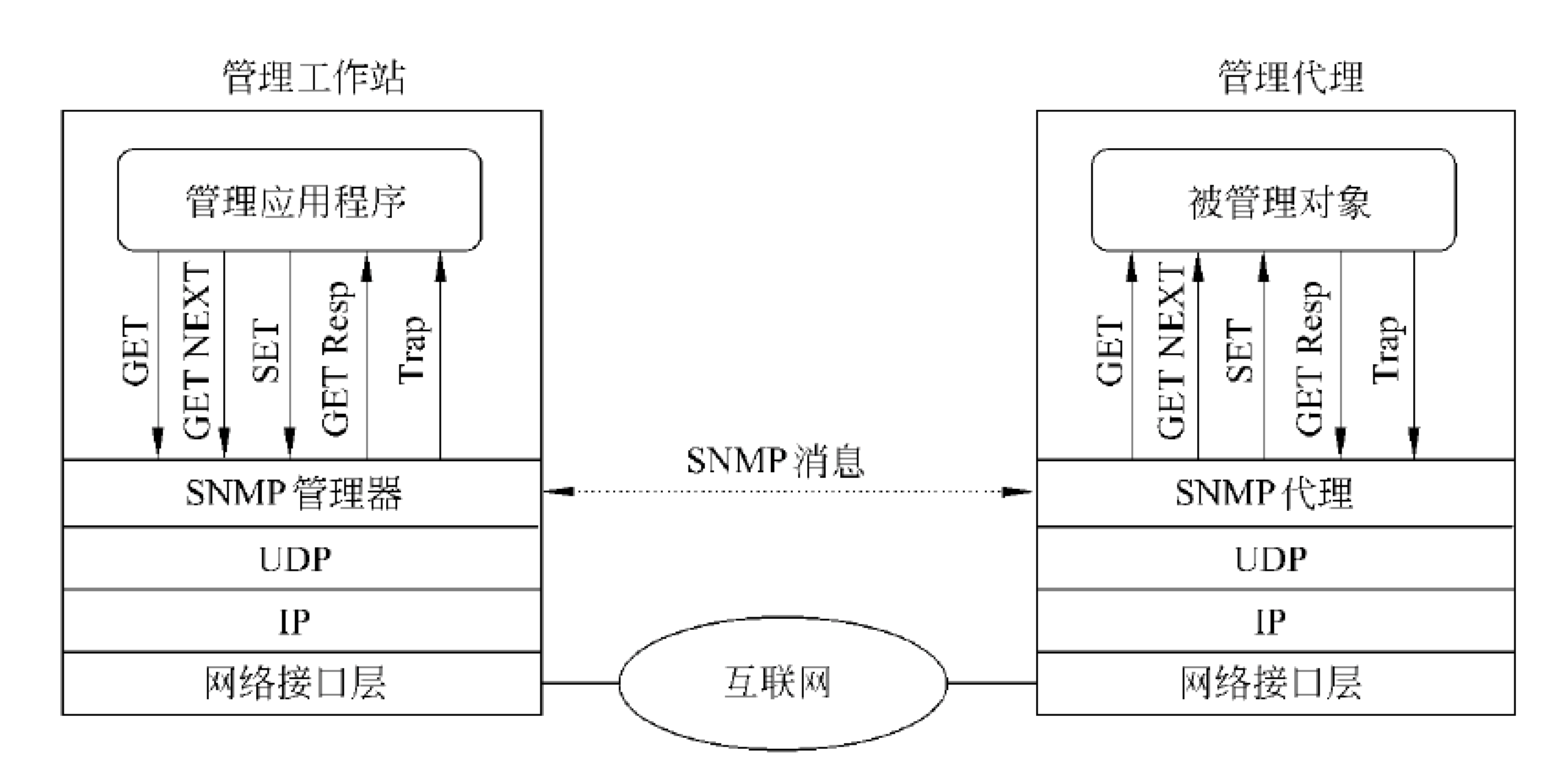


图 9.2 SNMP 作用过程

- GET Resp　是管理代理执行 GET 和 GET NEXT 命令后的响应,其中包含检索到的指定被管理对象相关的属性参数值;
- Trap　管理代理用于主动向网络管理工作站通报某个被管理对象发生的变化。

如果网络管理工作站查询某台交换机某个端口的状态(UP 或 DOWN,传输速率),网络管理工作站向指定交换机发送 SNMP GET 命令,命令中指定需要查询的被管理对象(端口号)和属性参数类型(工作状态和传输速率),包含该 SNMP 命令的 SNMP 消息到达交换机后,由交换机中的 SNMP 代理进行处理,SNMP 代理通过检索 MIB,找到指定被管理对象(交换机端口)的相关属性参数值(端口状态和传输速率),通过 SNMP GET Resp 命令将指定交换机端口的相关属性参数值发送给网络管理工作站,由管理应用程序以用户友好的界面显示出来。

同样,如果网络管理工作站需要配置某台交换机某个端口的状态(UP 或 DOWN,传输速率),网络管理工作站向指定交换机发送 SNMP SET 命令,命令中指定需要配置的被管理对象(端口号)和属性参数值(UP,100Mb/s),包含该 SNMP 命令的 SNMP 消息到达交换机后,由交换机中的 SNMP 代理进行处理,SNMP 代理将指定被管理对象(交换机端口)的相关属性参数值(端口状态和传输速率)设定为 UP 和 100Mb/s。

如果连接某台交换机某个端口的物理链路发生故障,该交换机管理代理将监测到该交换机端口状态发生变化(从 UP 转变为 DOWN),管理代理通过 Trap 命令主动向管理工作站通报这一情况。

9.1.3 SNMPv1 缺陷

1. 安全问题

必须保证只有授权的网络管理工作站才能通过 SNMP 命令对网络结点进行查询和配置,而且,允许将不同网络结点,或者同一网络结点的不同被管理对象授权给不同的网络管理工作站进行管理,因此,网络结点中的管理代理在执行 SNMP 命令之前,必须对命令的合法性进行检验,只允许执行已经授权对 SNMP 命令中指定的被管理对象进行指定操作的网络管理工作站发出的 SNMP 命令。

SNMPv1 通过共同体(Community)将对不同被管理对象的不同操作和授权网络管理工作站绑定在一起,如某个交换机可以设置如下有关被管理对象的访问权限:

访问权限 1	访问权限 2
共同体:aabb。	共同体:bbaa。
被管理对象:端口 1。	被管理对象:端口 1。
操作模式:只读。	操作模式:读写。

访问权限 1 表明允许共同体值为 aabb 的网络管理工作站通过 GET、GET NEXT 命令读取端口 1 的状态信息,如端口 1 连接的链路状态(UP 或 DOWN)、传输速率、经过端口 1 传输的字节数等。访问权限 2 表明允许共同体值为 bbaa 的网络管理工作站通过 GET、GET NEXT 命令读取端口 1 的状态信息,同时允许通过 SET 命令配置端口 1 的属性参数,如使能端口 1、端口 1 所属的 VLAN 等。从中可以看出,共同体等同于网络管理工作站用于查询、配置网络结点的通行证,由于 SNMPv1 直接用明文的方式在网络管理工作站和网络结点之间传输共同体,因此,很容易被第三方截获,任何攻击者一旦获得用于管理某个被管理对象的共同体,就可以对该被管理对象实施相应的操作,这将造成很大的网络安全隐患。

2. 集中管理的负荷问题

SNMPv1 支持集中式管理方式,如图 9.3(a)所示,网络管理工作站直接面向网络结点,周期性查询所有网络结点的状态,接收网络结点发送的 Trap 命令,以此产生整个网络的状态和流量分布信息,显然,这种管理方式下,网络管理工作站将成为性能瓶颈。图 9.3(b)中虽然使用了两个网络管理工作站,也只是将一个大的网络管理域分割为两个较小的网络管理域,两个网络管理工作站各自管理属于所负责的管理域的网络结点,网络管理员也只能分别通过每一个网络管理工作站对属于不同管理域的网络结点实施管理,每一个网络管理工作站只能提供和所管理的网络结点有关的状态和流量分布信息,如果想要得到整个网络的状态和流量分布信息,需要网络管理员对取自两个网络管理工作站的状态和流量分布信息进行综合处理。

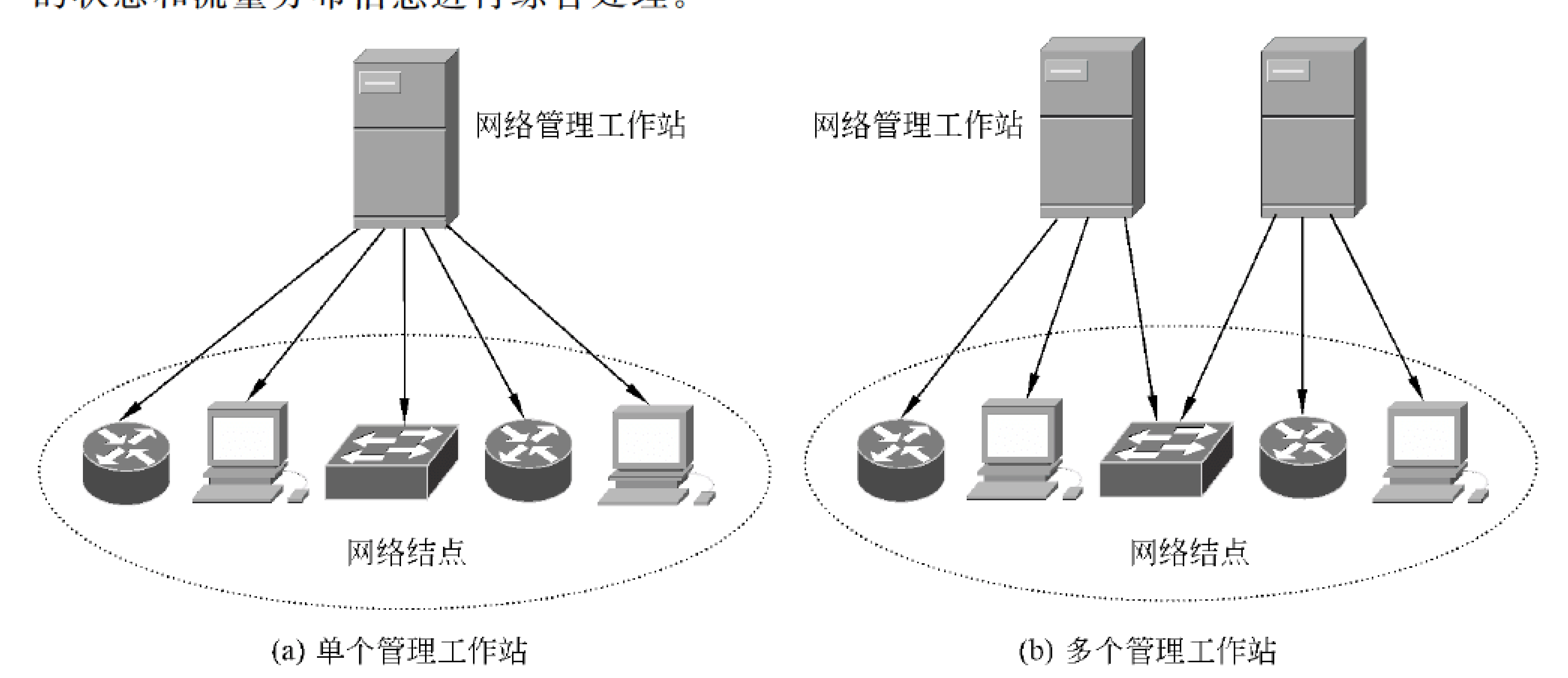


图 9.3 集中管理方式

真正解决大型网络的网络管理问题的机制是如图 9.4 所示的分布式管理方式，将一个大型网络分割为多个管理域，每一个网络管理工作站负责一个管理域，由中心网络管理工作站对网络管理工作站进行管理，这种分布式管理方式下，网络管理工作站具有双重功能，对于属于所负责的管理域的网络结点，实施网络管理工作站功能，对于中心网络管理工作站，实施管理代理功能，通常用委托代理称呼这种具有双重功能的设备。SNMPv1 并不支持分布式管理方式，因此，并不适合作为大型网络的网络管理协议。

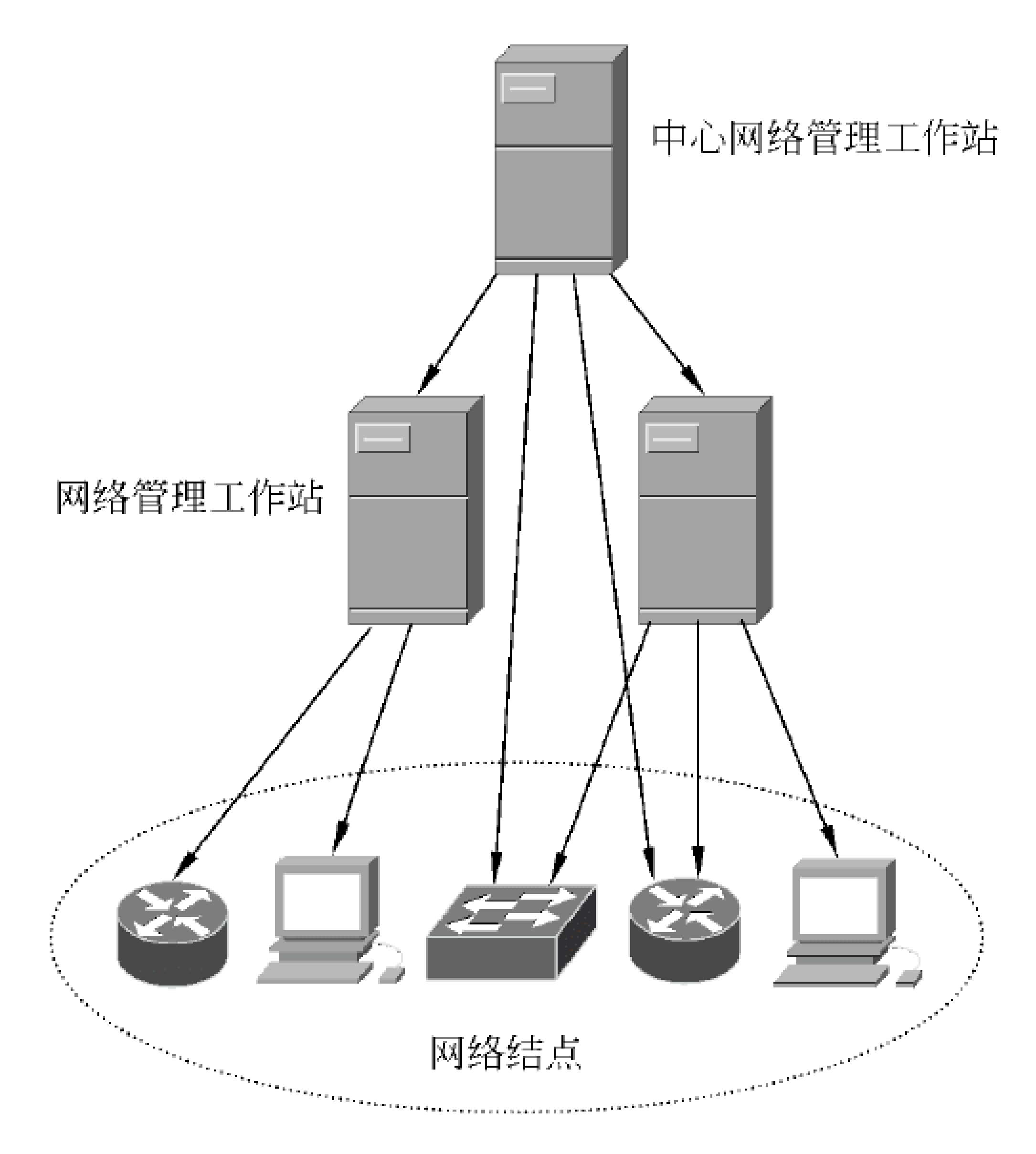


图 9.4　分布式管理方式

9.1.4　SNMPv3 的安全机制

由于网络管理工作站和网络结点之间通过 SNMP 消息实现查询和配置功能，因此，必须解决：

- 网络管理工作站的身份认证问题。防止攻击者冒用网络管理工作站查询网络结点状态、修改网络结点配置。
- SNMP 消息保密问题。防止攻击者通过截获 SNMP 消息来了解网络结点状态和配置。
- 防中继攻击（亦称重放攻击）问题。防止攻击者截获某个用于配置网络结点的 SNMP 消息，并在不适当的时间将其传输给网络结点。

1. 网络管理工作站身份认证机制

如果网络管理工作站和某个网络结点共享一个对称密钥 K，则网络结点认证网络管理工作站的身份过程就是确认 SNMP 消息发送者是否拥有对称密钥 K 的过程，用对称密钥 K 加密 SNMP 消息的报文摘要是最简单、开销最少的发送者身份认证机制，图 9.5 给出整个认证过程。

实际操作过程中用 HMAC-MD5-96 或 HMAC-SHA-1-96 同时完成报文摘要和加密运算过程，整个过程如图 9.6 所示。

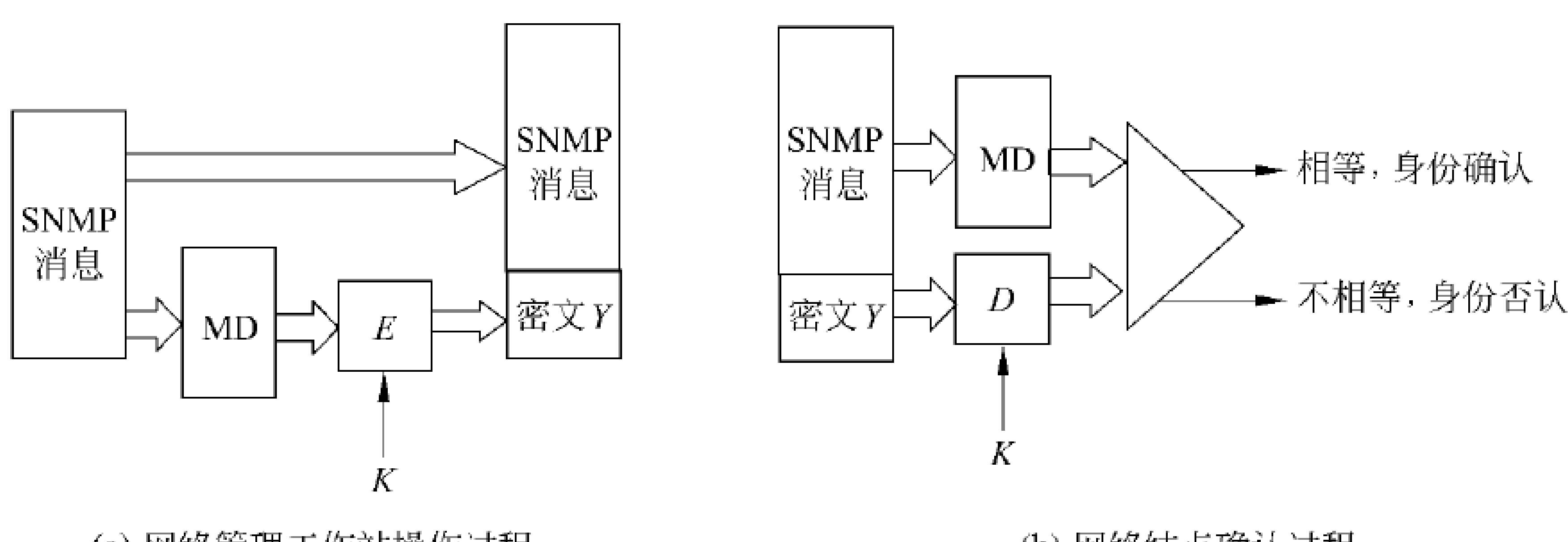


图 9.5 认证网络管理工作站身份过程

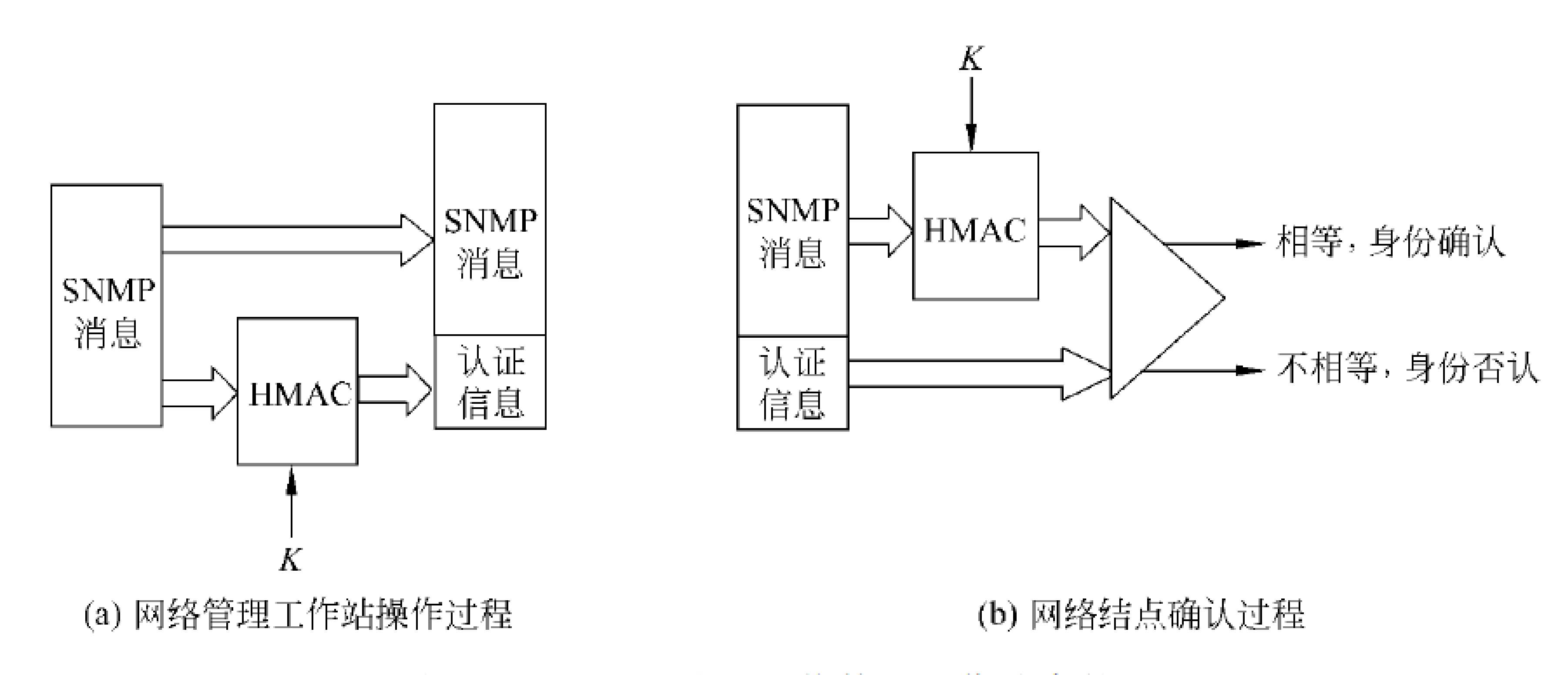


图 9.6 HMAC 认证网络管理工作站身份过程

当被管理对象状态发生变化时，网络结点中的管理代理可以通过 Trap 消息主动向网络管理工作站通报被管理对象变化后的状态，这种情况下，网络管理工作站需要认证网络结点的身份，以免攻击者冒充某个网络结点发送虚假的被管理对象状态信息。

2. SNMP 消息加密机制

SNMP 加密机制如图 9.7 所示，DES 作为加密算法，密钥长度为 56 位。

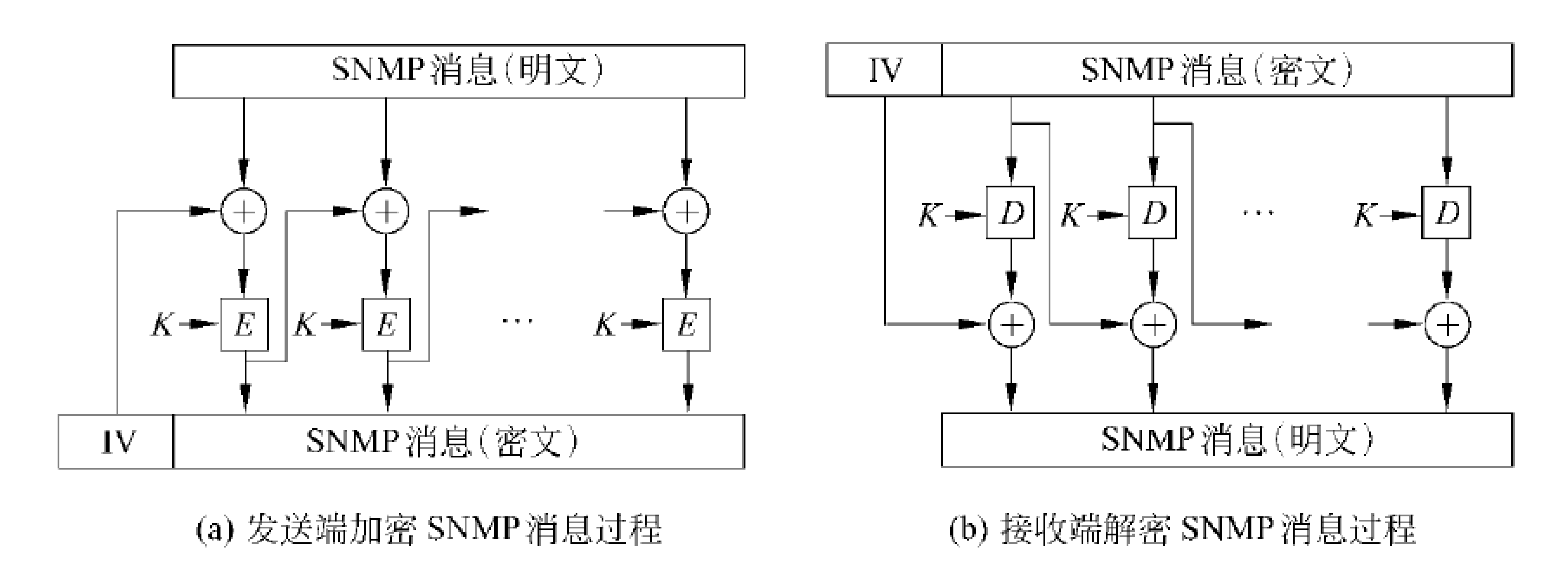


图 9.7 SNMP 消息加密机制

3. 防中继攻击机制

网络管理工作站和网络结点都保持两个本地计数器：32 位的引导计数器 boot 和 32 位的时间计数器 time，同时对每一个认证者保持四个变量：认证者名、32 位的认证者

引导计数器 Aboot、32 位的认证者时间计数器 Atime 和 32 位最新的认证者时间 Lastesttime，即来自认证者 SNMP 消息中最大的时间值。不同类型的 SNMP 消息，认证者是不同的，对于 GET、GET NEXT、SET 消息，执行这些命令的网络结点中的管理代理是认证者，对于 Trap 消息，接收该消息的网络管理工作站是认证者。SNMP 消息中除了用于认证发送者身份的认证信息、用于解密 SNMP 消息的初始向量(或初始向量种子)外，还需包含认证者名、引导计数器值和时间计数器值，对于发送给认证者的 SNMP 消息，如网络管理工作站发送给网络结点的 GET、GET NEXT、SET 消息，认证者名是对应网络结点名，引导计数器值和时间计数器值是网络管理工作站对应该网络结点保持的认证者引导计数器 Aboot 和认证者时间计数器 Atime 值。对于认证者发送的 SNMP 响应消息，如网络结点发送给网络管理工作站对应 GET、GET NEXT 的响应消息：GET Resp 消息，认证者名是该网络结点名，引导计数器值和时间计数器值是该网络结点保持的本地引导计数器 boot 和本地时间计数器 time 值。

当非认证者接收到 SNMP 消息，用 SNMP 消息给出的认证者名找到该认证者对应的三个参数：Aboot、Atime 和 Lastesttime，如果 SNMP 消息中给出的参数值是最新的，则用 SNMP 消息中给出的参数值取代原来的参数值，取代算法如图 9.8 所示。

```
IF 引导计数器值>Aboot.OR.(引导计数器值=Aboot.AND.时间计数器值>Lastesttime)
{
    Aboot=引导计数器值;
    Atime=时间计数器值;
    Lastesttime=时间计数器值;
}
```

图 9.8　取代算法

无论本地计数器值，还是和每一个认证者对应的计数器值都正常递增，每经过一秒，time＝time＋1，一旦 time 溢出，boot＝boot＋1。每经过一秒，Atime＝Atime＋1，一旦 Atime 溢出，Aboot＝Aboot＋1。

当认证者接收到 SNMP 消息，首先判别 SNMP 消息中给出的认证者名是否和自己相同，在相同的前提下，如果图 9.9 所示的条件成立，则确定该 SNMP 消息是中继攻击消息，予以丢弃。

```
IF boot=2^31-1.OR.引导计数器值≠boot.OR.(引导计数器值=boot.AND.
        ABS(时间计数器值-time)≥150))
```

图 9.9　中继攻击判别条件

图 9.9 所示的条件表明如果认证者本地引导计数器值 boot＝$2^{31}-1$，表明所有接收到的 SNMP 消息都是中继攻击消息。如果 SNMP 消息中给出的引导计数器值和认证者本地引导计数器值 boot 不同，确定接收到的 SNMP 消息是中继攻击消息。如果 SNMP 消息中给出的时间计数器值和认证者本地时间计数器值 time 之间差值大于±150，确定接收到的 SNMP 消息是中继攻击消息。

4. 密钥生成机制

一般情况下，一个网络管理工作站管理多个网络结点，如图 9.10 所示，这种管理模式

下，对于大多数 SNMP 消息，如 GET、GET NEXT、SET 消息，网络结点是认证者，负责对管理者身份进行认证，因此，网络管理工作站和每一个网络结点之间都需要两个对称密钥：认证密钥和加密密钥。当然，为了方便，网络管理工作站和所有网络结点之间可以使用同一对密钥，但一旦某个网络结点的密钥外泄，所有网络结点的管理安全都将成为问题，因此，为安全起见，网络管理工作站和不同的网络结点之间传输 SNMP 消息时，需要使用不同的密钥对。每一个认证密钥密钥长度或是 16 字节（使用 HMAC-MD5-96），或是 20 字节（使用 HMAC-SHA-1-96），加密密钥长度是 16 字节，其中 8 字节作为 DES 密钥，8 字节作为初始向量 IV（或者 IV 种子），由于实际的 DES 密钥是 56 位，因此，8 字节中的每一个字节的最高位是不用的。显然，由网络管理员记住这些密钥对是不现实的，但如果将这些密钥对存储在网络管理工作站中，又会造成安全隐患。实际的密钥生成机制如图 9.11 所示，网络管理员只需记住一对口令（认证口令和加密口令），每一个口令经过反复重复扩展为 2^{20} 字节长度，然后对扩展后产生的字符串进行 MD5 或 SHA-1 运算，产生 16 字节（MD5 运算）或 20 字节（SHA-1 运算）的用户密钥。对不同的认证者，首先将用户密钥和该认证者名串接为一个字符串，然后对该字符串进行 MD5 或 SHA-1 运算，产生 16 字节（MD5 运算）或 20 字节（SHA-1 运算）的认证者密钥，这样，可以通过一个口令衍生出多个对应不同认证者的认证者密钥，由于 MD5 或 SHA-1 运算都是单向运算，即无法通过运算结果推导出原始输入数据，因此，即使某个认证者密钥外泄，也无法通过该认证者密钥得出用户口令，因而无法得到其他认证者密钥，加密密钥的生成机制和认证密钥生成机制相同，但原始输入是加密口令。

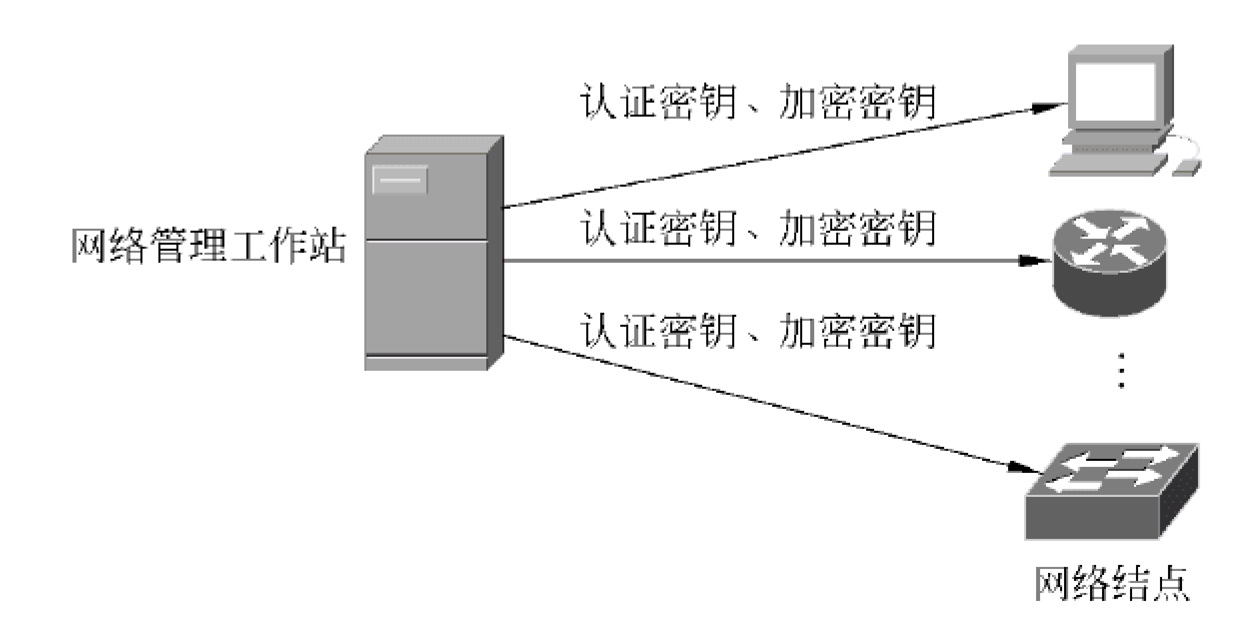


图 9.10 管理模式

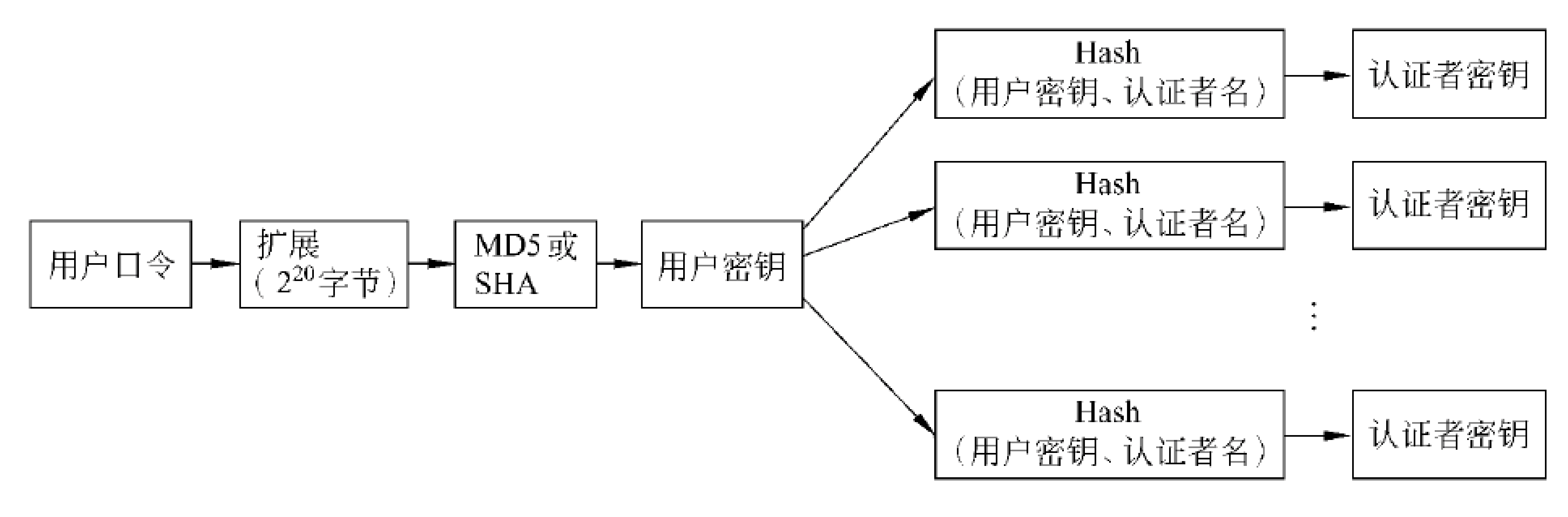


图 9.11 密钥生成机制

9.2 网络综合监测系统

在网络操作过程中,每一个网络结点都会记录下大量信息,这些信息是判别网络运行是否正常、网络性能是否能够满足应用需要、网络是否遭到黑客攻击的重要依据,但如图 9.12 所示,这些信息由不同的管理系统汇聚、处理,如 SNMP 网络管理工作站能够获得网络结点配置、状态信息和经过该网络结点传输的信息流分布情况,管理服务器能够获得探测器和主机入侵防御系统监测到的黑客攻击过程、非法访问资源过程及主机状态信息,但这些管理系统是相互独立的,如果想得到有关网络操作的完整信息,需要网络管理员人工集成由不同的管理系统汇聚、处理后的结果,对于一个大型网络,通过人工集成由不同的管理系统汇聚、处理后的结果,得出有关网络操作的完整信息的难度是无法想象的,因此,需要一个能够监测到网络中发生的一切事情,并就其对网络安全的影响进行自动评估的网络综合监测系统。

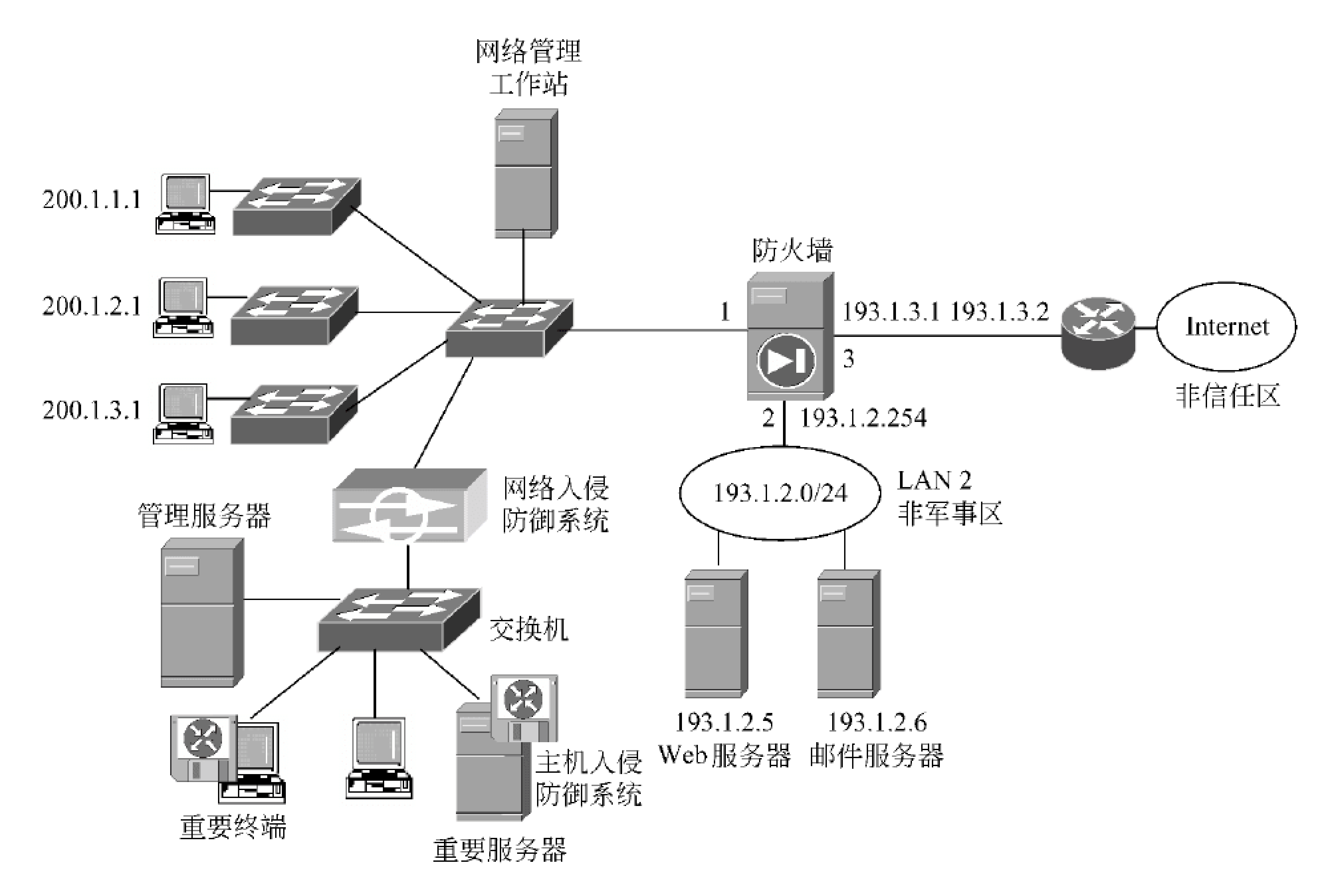


图 9.12 网络系统结构

9.2.1 网络综合监测系统功能

网络综合监测系统功能主要有两个：一是监测网络上发生的一切事情,二是评估这些事情对网络安全的影响。具体完成的工作有：

- 获悉网络中有哪些网络设备、哪些服务器、提供哪些网络服务；
- 获悉网络中资源访问模式和信息流分布情况；
- 获悉用户从 Internet 下载的新的应用程序；

- 获悉终端和服务器所使用的系统软件和应用软件的类型和版本；
- 发现攻击行为，跟踪攻击源头；
- 主动提示网络存在的安全漏洞；
- 跟踪终端和服务器的安全状态；
- 确定非法访问网络资源的用户；
- 以友好的图形界面方式实时提供网络状态，可以通过关联查找方式获取相关信息。

9.2.2 网络综合监测系统实现机制

1. 主动探测机制

许多攻击利用操作系统漏洞实现，不同类型、版本的操作系统可能存在不同的漏洞，需要用不同的补丁软件解决，因此，确定终端和服务器所运行的操作系统类型、版本，针对发现的漏洞及时下载对应补丁软件是确保终端和服务器安全的重要步骤。主机入侵防御系统具有检测主机系统所运行的操作系统类型、版本的功能，并将检测结果通报给网络综合监测系统。由于成本因素，大量主机系统没有安装主机入侵防御系统，这些主机系统所使用的操作系统类型、版本或者由用户主动向网络综合监测系统通报，或者由网络综合监测系统进行探测。对于一个具有成千上万用户且用户不断变化的大型网络，第一种方法显然不可行，因此，往往采用网络综合监测系统探测机制，如果这种探测过程由网络综合监测系统主动发起，称为主动探测机制。

由于不同类型、版本的操作系统在 TCP/IP 协议栈的实现细节上存在差别，只要掌握了这种差别，且能够检测出某个主机系统所运行的操作系统 TCP/IP 协议栈的实现细节，就可推测该操作系统的类型、版本。不同类型、版本的操作系统在 TCP/IP 协议栈的实现细节上的差别主要有如下这些。

- 侦听端口对置位 FIN 位 TCP 报文的反应：不同类型、版本的操作系统对侦听端口接收到的不属于任何已经建立的 TCP 连接且 FIN 位置位的 TCP 报文的反应是不同的，一种反应是不予理睬，一种反应是回送一个 FIN 和 ACK 位置位的响应报文，如 Windows NT/2000/2003。
- 侦听端口对存在无效标志位的 SYN 报文的反应：正常的 TCP 连接建立过程是三次握手过程，即请求方首先发送一个置位 SYN 位的请求报文，侦听方回送一个置位 SYN 和 ACK 位的响应报文，请求方发送一个置位 ACK 的确认报文。如果请求方发送的请求报文不仅置位 SYN 位，还置位了其他标志位，不同类型、版本的操作系统对这种请求报文的反应是不同的，一种反应是将其作为错误请求报文予以丢弃，一种反应是回送一个不仅 SYN 和 ACK 位置位，而且同样置位请求报文中置位的无效标志位的响应报文，如 Linux。
- 不同的初始序号(ISN)：不同类型、版本的操作系统接收到请求方发送的 TCP 连接请求报文后，在回送的 TCP 连接响应报文中给出的初始序号(ISN)值是不同的。
- 不同的初始窗口值：不同类型、版本的操作系统接收到请求方发送的 TCP 连接请

求报文后，在回送的 TCP 连接响应报文中给出的初始窗口值是不同的。

- 封装 TCP 报文的 IP 分组的 DF 位：不同类型、版本的操作系统对封装 TCP 报文的 IP 分组的 DF 位的处理方式不同，有些操作系统为了改善网络传输性能，一律将封装 TCP 报文的 IP 分组的 DF 位置位，不允许转发结点拆分封装 TCP 报文的 IP 分组。
- ICMP 出错消息的频率限制：不同类型、版本的操作系统对发送 ICMP 出错消息的频率有着不同的限制，通过向某个主机系统连续发送一些确定是无法送达的 UDP 报文，如一些接收端口号为高编号的 UDP 报文，然后对在给定时间内回送的“目的地无法到达”的 ICMP 出错消息进行统计，得出该主机系统 ICMP 出错消息的频率限制。
- ICMP 消息内容：不同类型、版本的操作系统在 ICMP 返回消息里给出的文字内容是不一样的。

2. 被动探测机制

主动探测机制需要网络综合监测系统向主机系统发送探测报文，然后根据主机系统回送的响应报文来推测主机系统所运行的操作系统类型和版本，当网络规模很大时，这种探测机制的成本会很高，实际上，分布在网络中的探测器也可以通过检测不同主机系统发送的 IP 分组来推测主机系统所运行的操作系统类型和版本，不同类型和版本的操作系统往往在下述字段的设置上有所区别：

- IP 分组 TTL 字段值；
- TCP 窗口字段值；
- IP 分组 DF 标志位。

分布在网络中的探测器通过综合分析 IP 分组中的上述字段值，来推测该主机系统所运行的操作系统类型和版本。

3. 集成 SNMP 网络管理系统

网络结点中的管理代理可以提供任意两个主机之间的流量、应用层协议分布，对于路由器和交换机，可以提供每一个端口的状态、传输效率，特定主机发送的分组数和字节数，属于不同应用层协议的报文数和字节数，因为输出队列溢出而丢弃的报文数和字节数，根据这些信息，可以了解网络中每一个网段的流量分布情况，任意两个主机之间传输的、和特定应用层协议相关的报文数、字节数，特定主机占用网络中各个网段带宽的情况，属于不同应用层协议的报文在总的流量中所占的比例，整个网络的连通情况，拥塞状态，性能瓶颈，信息流模式和流量变化过程等。

4. 集成防火墙功能

防火墙主要作用于内部网络和 Internet 的边界，用于检测和控制内部网络和 Internet 之间传输的信息流，因此，防火墙能够检测到内部网络终端从 Internet 下载的应用程序、下载网页中隐藏的病毒、Internet 对内部网络终端实施的攻击、内部网络终端访问 Internet 资源模式、内部网络和 Internet 之间流量中不同应用层协议的比例、内部网络终端的扫描频率、端口扫描频率等。

5. 集成入侵防御系统功能

主机入侵防御系统可以提供主机系统所运行的操作系统类型和版本、是否安装补丁软件、是否感染病毒、主机系统的安全状态、主机系统运行的应用程序等，网络入侵防御系统（主要为探测器）可以提供异常信息流模式和源头、异常信息流可能实施的攻击、异常信息流的攻击目标等。

6. 策略配置和关联检索

网络综合监测系统获取的信息是巨大的，为了有针对性地解决某个安全问题，需要主动探测机制、SNMP 管理系统、防火墙和入侵防御系统采集和通报特定的信息，安全策略就用于这些系统设置过滤表达式或信息采集、通报策略。为了在庞大的信息库中检索出和特定安全问题相关的信息，需要网络综合监测系统提供关联检索功能。

9.2.3 网络综合监测系统应用实例

1. 监测网络安全漏洞

黑客的许多攻击是利用主机操作系统或应用程序漏洞实现的，许多安全监测机构会定期公布当前流行的操作系统和应用程序的漏洞，软件厂家通过及时发布补丁软件来应对被发现的漏洞，黑客也会推出利用漏洞实施攻击的黑客软件，这是一个软件厂家和黑客之间抢时间、比速度的竞争游戏，一旦某个安全监测机构公布了某种操作系统或应用程序的漏洞，运行存在漏洞的软件的主机系统，在该主机系统更换存在漏洞的软件或运行该软件厂家发布的补丁软件前，是不安全的主机系统，这样的主机系统极易遭受黑客攻击，并因此使整个内部网络成为黑客攻击的牺牲品，因此需要检测出这种存在安全隐患的主机系统并加以隔离，具体步骤如下：

1）配置安全策略

网络综合监测系统及时下载安全监测机构最新公布的存在漏洞的操作系统或应用程序类型、版本，并在安全策略中禁止运行存在漏洞的主机系统继续访问 Internet。

2）SNMP 代理通报新发现的主机

网络结点，如交换机中的 SNMP 代理每发现一个新的主机系统，就主动向网络综合监测系统通报该主机系统的 IP 地址和 MAC 地址，为了精确起见，只有在网络结点中的接入端口（连接终端或服务器的端口）发现新的主机系统时，才启动主动通报功能。

3）探测该主机所运行的操作系统或应用程序类型和版本

网络综合监测系统通过主动探测机制获取该主机所运行的操作系统或应用程序类型和版本，一旦和某个存在安全漏洞的软件匹配，进行 4）指出的隔离操作。

4）隔离操作

如果网络系统如图 9.13 所示，IP 地址为 200.1.1.1、MAC 地址为 MAC 1 的主机系统所运行的操作系统类型和版本存在漏洞，网络综合监测系统在防火墙端口 1 输入方向设置过滤规则：源 MAC 地址＝MAC 1 丢弃。

在防火墙端口 1 输出方向设置过滤规则：目的 MAC 地址＝MAC 1 丢弃。

这样，保证该主机系统在更换操作系统前，或在下载并运行补丁软件前，无法和

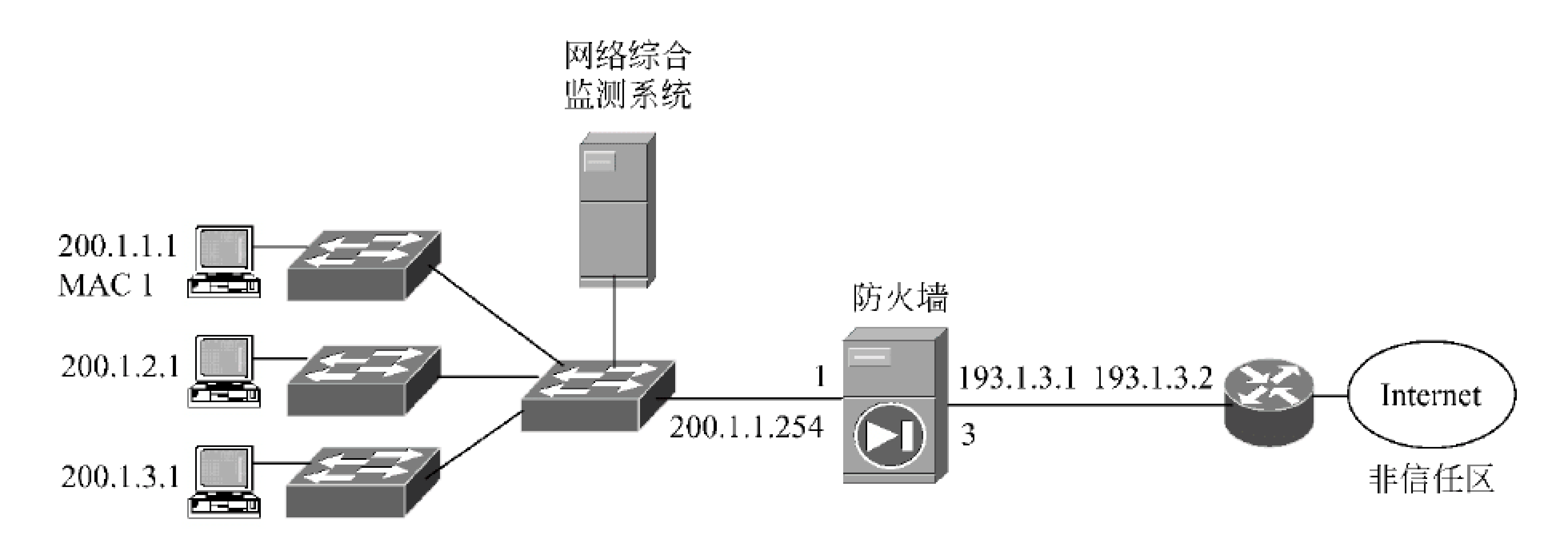


图 9.13　隔离操作过程

Internet 中的终端进行通信，避免因此遭到攻击。之所以选择用 MAC 地址作为用于匹配过滤规则的字段值是因为在主机通过 DHCP 自动获取配置信息的情况下，IP 地址是变化的。

2. 禁止访问非法网站

非法网站是指内容不健康或者经常传播网络病毒的网站，如果觉察到内部网络用户访问这样的网站，需要立即将该用户终端从网络中断开。

1) 配置安全策略

网络综合监测系统及时下载或手工配置非法网站的统一资源定位符(URL)列表，并在安全策略中规定：将访问属于非法 URL 列表中网页的用户终端从网络中断开。

2) 防火墙通报 HTTP 请求报文

防火墙一旦检测到内部网络终端发送的 HTTP 请求报文，在按照访问控制策略转发该 HTTP 请求报文的同时，按照网络综合监测系统的要求将 HTTP 请求报文中的关键字段值，如 URL、FROM、TO、封装 HTTP 请求报文的 IP 分组的源和目的地址等，发送给网络综合监测系统，网络综合监测系统用 HTTP 请求报文的 URL 匹配非法 URL 列表，一旦非法 URL 列表中存在和该 URL 相同的项，进行 3)、4)指定的操作。

3) 定位该用户终端

在进行断开操作前，必须定位该用户终端，即找出该用户终端所连接的交换机端口，由于网络综合监测系统只得到用户终端的 IP 地址，需要确定连接该 IP 地址指定子网的交换机，根据交换机中 IP 地址和 MAC 地址的绑定关系、交换机中站表内容及内部网络拓扑结构图确定连接该用户终端的交换机端口。

4) 断开操作

通过向该交换机发送 SNMP SET 命令，将连接用户终端的交换机端口由 UP 改为 DOWN，同时通过其他途径向该用户发出警告。

3. 监测蠕虫病毒传播过程

蠕虫病毒的特点是能够自动传播，一旦某个主机系统感染了蠕虫病毒，蠕虫病毒能够通过主机和端口扫描发现其他存在漏洞的主机系统，并将自己传播给它，这是蠕虫病毒能够快速蔓延的原因，Blaster 蠕虫病毒利用 Windows 远程过程调用(Remote Procedure

Call,RPC)机制中的漏洞进行传播。RPC 机制允许某台主机系统上运行的程序能够无缝执行另一台主机系统上的代码,许多资源共享服务需要用到这一机制,如局域网中用户之间的文件共享服务,因此,内部网络中的主机系统往往启用这一机制,这就为 Blaster 蠕虫病毒的传播提供了平台。

1) 网络入侵防御系统监测端口扫描侦察

不同 RPC 服务侦听的端口是不一样的,不同主机系统打开的 RPC 服务也不同,因此,攻击主机传播蠕虫病毒的第一步是对网络中其他主机系统进行端口扫描。当网络入侵防御系统(探测器)监测到某个主机正在实施端口扫描,将其 IP 地址、被扫描的主机 IP 地址和端口号集合通报给网络综合监测系统。

2) 定位攻击主机

根据攻击主机的 IP 地址确定攻击主机位于 Internet 或内部网络,对位于内部网络的攻击主机,根据 SNMP 管理系统获得的信息,确定连接该主机的交换机端口,通过向该交换机发送 SNMP SET 命令将该交换机端口由 UP 改为 DOWN,以此将该攻击主机从网络上断开,同时通过其他途径向该主机用户发出警告。如果主机位于 Internet,通过设置边界防火墙,禁止该攻击主机和内部网络中的终端进行通信。

3) 发出安全警告

在监测到网络中发生 Blaster 蠕虫病毒攻击的情况下,通过主动探测机制获取被攻击主机系统是否打开 RPC 服务,并对这些主机系统发出警告,要求对主机系统进行检测,判别是否感染 Blaster 蠕虫病毒。

4) 加强内部网络安全监测

通过修改内部网络探测器中的监测策略,加强对 Blaster 蠕虫病毒攻击的监测,如端口扫描监测、Blaster 蠕虫病毒特征匹配等,将 Blaster 蠕虫病毒攻击消灭在萌芽。

4. 监测网络性能瓶颈

网络性能出现瓶颈主要指内部网络中的某个网络结点或某段链路出现过载现象,导致大量经过该网络结点或网络链路传输的数据被丢弃。

1) 监测过载结点

网络结点中的管理代理能够采集每一个端口的工作情况,如指定时间段内该端口接收、发送的 MAC 帧数、字节数、IP 分组数,指定时间段内端口输出队列平均长度、因为输出队列溢出而丢弃的 MAC 帧数、字节数、IP 分组数,还允许为这些工作参数设置阈值,管理代理一旦发现从某个端口采集的工作参数超过阈值,则通过 Trap 命令将这种情况主动通报给网络综合监测系统。

2) 分析流量组成

通过 SNMP 网络管理系统可以得到经过拥挤网络结点的流量中各个源终端的分布情况、各种应用层协议的分布情况,综合内部网络中其他网络结点采集的流量信息,可以得出流量突然增大的网络终端的流量变化情况、流量中各种应用层协议的分布情况,根据网络入侵防御系统统计到的基准信息,计算出流量变化超出设定范围的网络终端及对应的应用层协议。

3）限制终端流量

定位这些源终端的位置和源终端至监测到的拥挤网络结点的传输路径，在传输路径经过的某个具有限制输入流量功能的端口设置限速器，设定该终端各种应用层协议所对应的最大流量，一旦超过设定流量，将丢弃超过流量的后续数据。

习　　题

9.1　简述 SNMP 的主要功能。

9.2　列出常见的配置网络结点的机制，并比较它们的优缺点。

9.3　如何了解整个网络的状态和流量分布？

9.4　根据如图 9.14 所示的网络结构，给出通过网络管理工作站看到的有关终端 A 的信息。

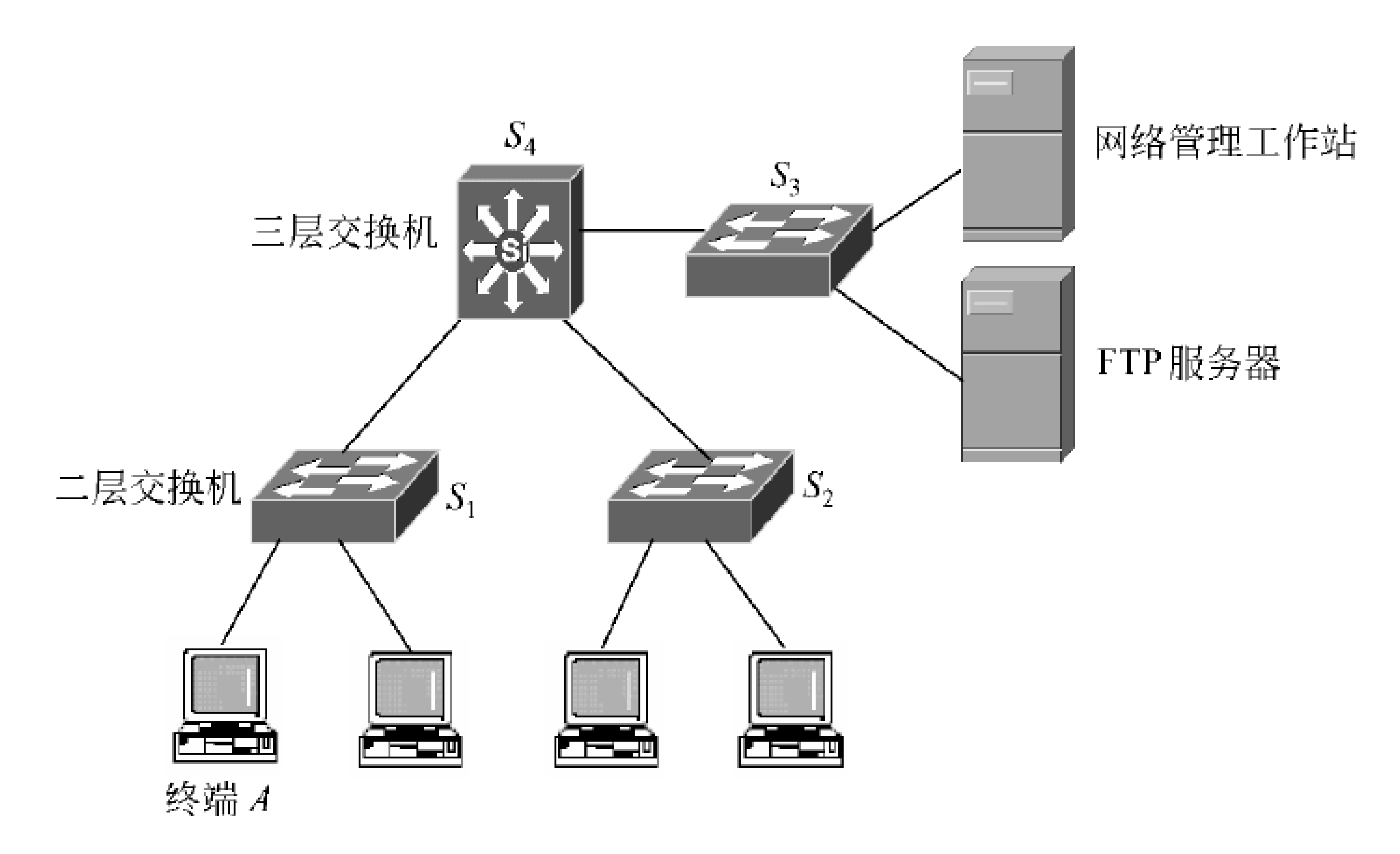


图 9.14　题 9.4 图

9.5　网络结构如图 9.14 所示，如何通过网络管理工作站给出的有关终端 A 的信息确定终端 A 因为感染蠕虫病毒正在向网络的其他终端发起攻击？

9.6　SNMPv1 的安全隐患是什么？黑客如何利用这些安全隐患实施攻击？

9.7　根据如图 9.14 所示的网络结构，给出黑客利用 SNMPv1 安全隐患控制网络工作过程的思路。

9.8　SNMPv3 解决 SNMPv1 安全隐患的方法是什么？

9.9　根据如图 9.14 所示的网络结构，解释网络管理工作站对网络结点实施安全配置的原理。

9.10　实现网络综合监测系统的困难是什么？如何解决？

9.11　网络结构如图 9.15 所示，给出网络综合监测系统实现下述控制过程的思路。

- 防止终端 A 下载包含病毒的网页；

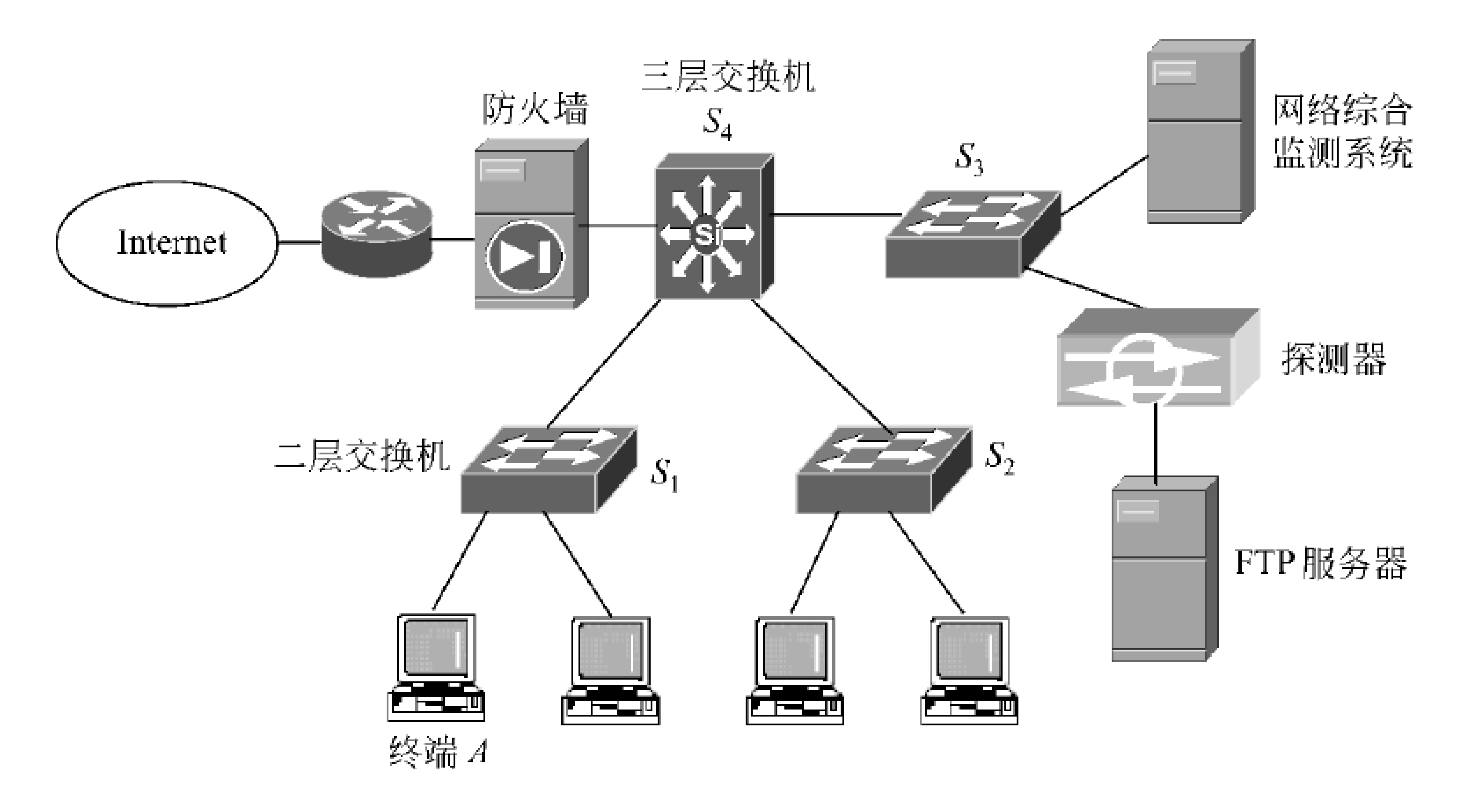


图 9.15 题 9.11 图

- 确定终端 A 被安装了木马程序;
- 确定对 FTP 服务器实施 SYN 泛洪攻击的攻击源;
- 阻止某个终端通过大量发送 ICMP ECHO 请求报文阻塞网络链路。

第10章 安全网络设计实例

CHAPTER

10.1 安全网络概述

10.1.1 安全网络设计目标

网络作为信息系统的基础设施，其最终目标是保障信息的适用性、保密性、完整性、不可抵赖性和可控制性。安全网络作为安全信息系统的一个重要组成部分，其设计目标是保证网络具有如下功能：

- 能够有效防御来自内部和外部的攻击；
- 能够对网络资源的访问过程实施有效控制；
- 能够对用户行为进行有效监控；
- 能够对网络运行状态进行实时监测；
- 能够对网络性能变化过程和原因进行跟踪、分析；
- 能够安全传输机密信息。

10.1.2 安全网络主要构件

为了实现安全网络的功能，安全网络必须包含如下和实现网络安全功能相关的构件：

- 接入控制和认证构件。接入交换机中必须包含用于对接入用户身份进行认证，对用户终端接入过程实施控制的构件。
- 分组过滤和速率限制构件。接入交换机和路由器中必须包含用于控制信息流传输的分组过滤构件，和对接入终端的实际传输速率进行控制的速率限制构件。
- 防火墙。在内部网络和外部网络(通常为 Internet)边界必须设置实施访问控制策略的防火墙设备。
- 入侵防御系统。为保障网络的适用性，必须对重要网络资源实施安全保护。由于目前黑客攻击手段的多样性，如攻击源可能来自内部或外部网络，采用的攻击机制可能未被发现，因此，需要用入侵防御系统对发送给受重点保护的网络资源的信息流进行异常检测，以免这些网络资源遭受攻击。

- VPN 接入构件。出差在外的企业员工可能需要通过 Internet 访问企业内部网络资源，为了保证这种访问过程的安全性，需要通过 VPN 技术接入内部网络，因此，内部网络连接外部网络的边界设备(通常为防火墙)需要包含 VPN 接入构件。
- 认证、管理和控制服务器。整个网络的接入认证信息、管理信息和安全策略可以分布在多个安全构件中，也可以统一存储在相应的服务器中。统一配置接入认证信息、管理信息和安全策略可以方便用户接入，减少网络管理员的工作量，统一各种网络安全构件的配置。

10.1.3 网络资源

构建安全网络的目标是保护网络资源免遭攻击。安全网络具有如下网络资源：

- 网络设备。如路由器、交换机、防火墙等。
- 网络操作信息。实现正常信息传输所需要的一些信息，如路由表、访问控制策略表、访问控制列表等。
- 链路带宽。
- 主机系统。包括主机系统的硬件和软件资源、存储在主机系统中的文件、数据库等。
- 在网络中传输的信息。信息资源除了存储在主机系统中的信息、网络设备中的操作信息外，还应包含正在网络中传输的信息。
- 用户私密信息。如用户身份、账号、口令、加密信息用的密钥等。

10.1.4 安全网络设计步骤

1. 确定需要保护的网络资源

对所有网络资源都实施保护是不现实的，因为保护网络资源需要成本，因此，只能对网络中重要且容易遭受攻击的网络资源实施保护，如数据库、Web 服务器等。需要指出的是，面向不同应用的网络，需要重点保护的网络资源是不同的。

2. 分析可能遭受的攻击类型

知己知彼，百战不殆，在设计安全网络前，必须分析网络可能遭受的攻击，不同应用特点的网络可能引发不同攻击者的注意，因而遭受的攻击类型也有所不同，常见的攻击类型如下：

- 非法访问，篡改网络信息。未经授权，非法访问，甚至篡改主机系统存储的信息、经过网络传输的信息、网络结点中的操作信息。
- 拒绝服务。通过非法占用带宽，过度消耗网络结点服务能力，使网络丧失对正常用户的服务功能。

3. 风险评估

风险评估主要从以下两方面着手：

- 网络被攻击成功的可能性。对应不同攻击类型和网络资源分布，预估网络遭受不同类型的攻击的可能性和被攻击成功的概率。
- 攻击成功可能造成的损失。针对网络应用特点和资源分布，假定某个攻击成功，

评估因攻击成功而造成的损失。

安全网络的最终目标是信息的适用性、保密性和完整性，如果风险评估结果表明一些攻击将最终导致网络无法保证安全目标的实现，那么，必须采取措施避免这种情况发生，因此，风险评估使得安全网络的具体设计过程变得有的放矢。

4. 设计网络安全策略

针对风险评估结果和特定攻击过程分析，制定网络安全策略，它由能够防御和抑制网络攻击的网络资源访问策略、信息传输模式、网络结点操作规则等组成，如以下例子：

- 不允许外部网络终端发起对内部网络终端的访问过程，但允许外部网络终端访问非军事区中的 Web 服务器；
- 不允许远程登录用户修改注册表等系统配置信息；
- 不允许某个内部网络终端在固定时间段内的平均流量超过 3Mb/s；
- 建立内部网络中关键网段的流量统计信息，监测流量变化过程；
- 连接在外部网络的终端必须通过 VPN 接入内部网络，完成身份认证后才能访问内部网络资源。

5. 实现网络安全策略

制定安全策略后，需要选择并在网络中合理设置网络安全构件，如防火墙、入侵防御系统、带有接入认证功能的交换机等，以此实现安全策略要求的访问控制功能和信息传输模式。

6. 分析和改进网络安全策略

根据安全网络结构和网络应用特点，分析安全策略对网络资源的保护力度，判断是否能够在遭受多种网络攻击的情况下，保证网络资源的适用性、保密性和完整性，如果发现存在安全漏洞，重新修改网络安全策略，这种过程可能需要反复多次，即使在安全网络实施后，也需要根据网络运行过程中发现的问题，有针对性地修改安全策略，并因此调整安全网络构件的设置和配置。

10.2　安全网络设计和分析

10.2.1　安全网络系统结构

安全网络系统结构如图 10.1 所示，它由一般网络构件和安全网络构件两部分组成。一般网络构件是指构成信息资源子网和信息传输子网的构件，如交换机、路由器、传输链路、主机系统（包括终端和服务器）等，安全网络构件是指实施网络安全策略的构件，如防火墙、入侵防御系统、VPN 接入设备等，目前交换机和路由器也内嵌安全网络构件，如实现接入控制、分组过滤、速率限制的构件。整个网络分成三部分：内部网络、非军事区和外部网络（Internet），内部网络也称信任区，外部网络也称非信任区，由防火墙将这三个区连成一个整体。出差在外的内部员工可以通过外部网络（Internet）访问内部网络中的 FTP 服务器，但需要通过采用 VPN 技术的第 2 层隧道接入内部网络，并由 VPN 接入设备（防火墙）完成接入用户的身份认证。内部网络使用本地 IP 地址，因此，连接内部网络

的防火墙端口启动 NAT 功能，来自内部网络的信息经过防火墙转发给外部网络前，须完成本地 IP 地址至全球 IP 地址的转换，反之亦然。

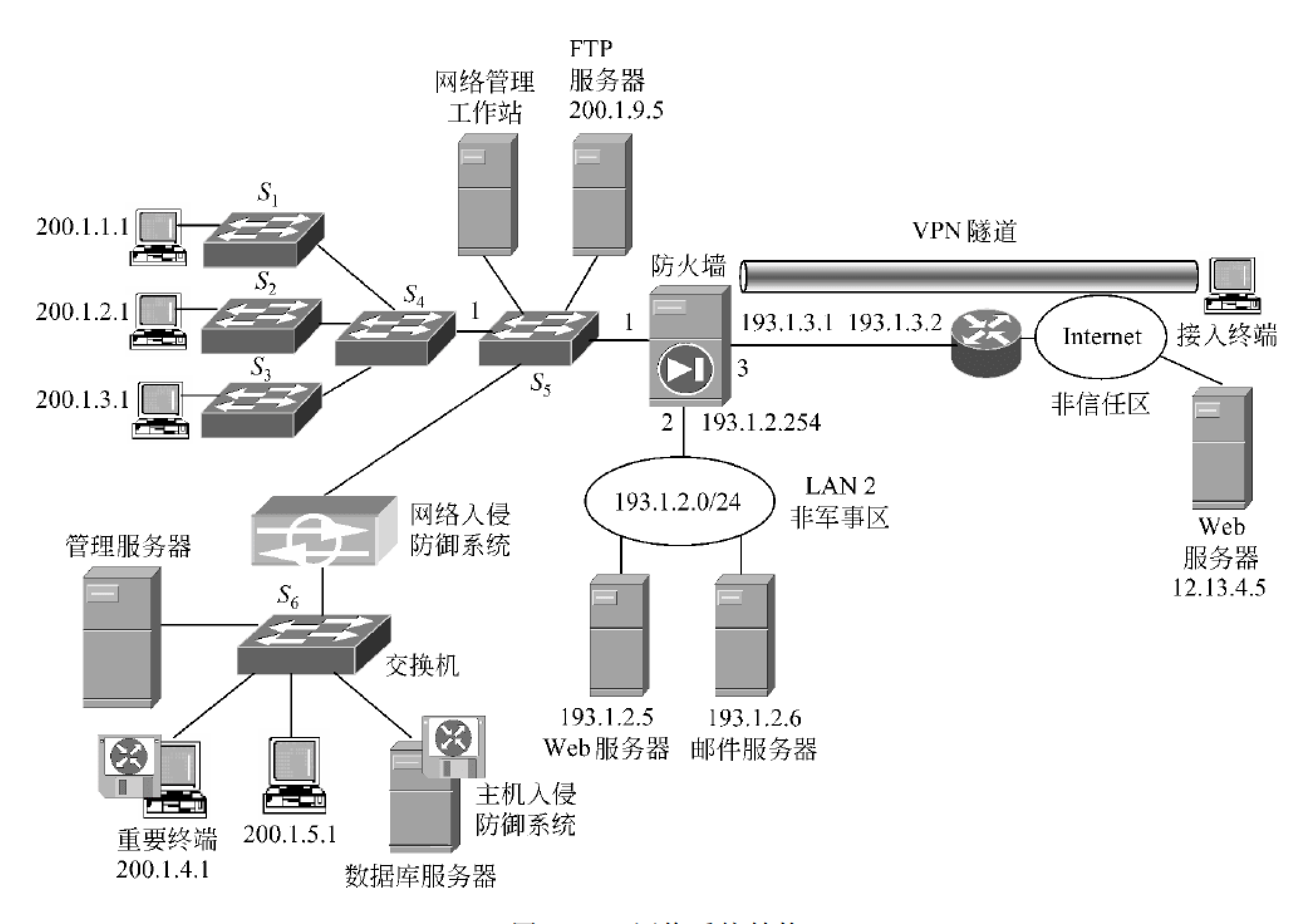


图 10.1 网络系统结构

10.2.2 网络安全策略

为了实现安全目标，制定下述安全策略：

- 允许内部网络终端对 Internet 的访问，但只能访问外部网络中的 Web 和 FTP 服务器；
- 允许内部网络终端对非军事区中的 Web 和 E-mail 服务器的访问；
- 允许外部网络（非信任区）终端对非军事区中的 Web 和 E-mail 服务器的访问；
- 只允许内部网络终端访问内部网络中的服务器，但允许内部员工通过第 2 层隧道经外部网络访问内部网络中的 FTP 服务器；
- 内部网络终端接入内部网络时须经身份认证；
- 内部网络终端的平均传输速率和峰值传输速率分别限制为 3Mb/s 和 5Mb/s；
- 不允许以交互方式访问内部网络的数据库服务器；
- 能够监测对内部网络数据库服务器发起的攻击；
- 内部网络使用本地 IP 地址，非军事区服务器使用全球 IP 地址，内部网络结构对外部网络终端是不可见的。

10.2.3　网络安全策略实现机制

1．交换机接入控制和速率限制机制

交换机 S_5 选择支持 802.1X 身份认证协议和端口速率限制的交换机类型，端口 1 使能 802.1X 身份认证和动态配置速率限制的机制，为了简单起见，假定交换机 S_5 进行本地认证。首先在交换机 S_5 中配置如表 10.1 所示的接入控制策略。

表 10.1　交换机 S_5 配置的接入控制策略

用户名	口令	认证机制	接入控制	平均速率/Mb/s	峰值速率/Mb/s
用户 *A*	PASSA	EAP-CHAP	允许	3	5
用户 *B*	PASS*B*	EAP-CHAP	允许	3	5
		⋮			

当交换机 S_5 配置了如表 10.1 所示的接入控制策略后，交换机 S_5 端口 1 的默认工作状态是阻塞，除了访问控制列表明确指明允许转发的 MAC 帧，其他从端口 1 接收到的 MAC 帧一律予以丢弃。某个内部网络终端希望接入内部网络并经内部网络访问内部网络或外部网络资源时，需要启动 802.1X 客户软件，终端一旦启动 802.1X 客户软件，开始图 10.2 所示的用户身份认证过程。在完成用户身份认证后，交换机 S_5 在端口 1 的访问控制列表中添加一项：

源 MAC 地址＝MAC *A*　允许转发　平均速率＝3Mb/s　峰值速率＝5Mb/s

其中，MAC *A* 是用户名为用户 *A* 的接入终端的 MAC 地址，该项信息表明允许转发所有从端口 1 接收到的源 MAC 地址＝MAC *A* 的 MAC 帧，但传输速率必须受平均和峰值速率的限制。

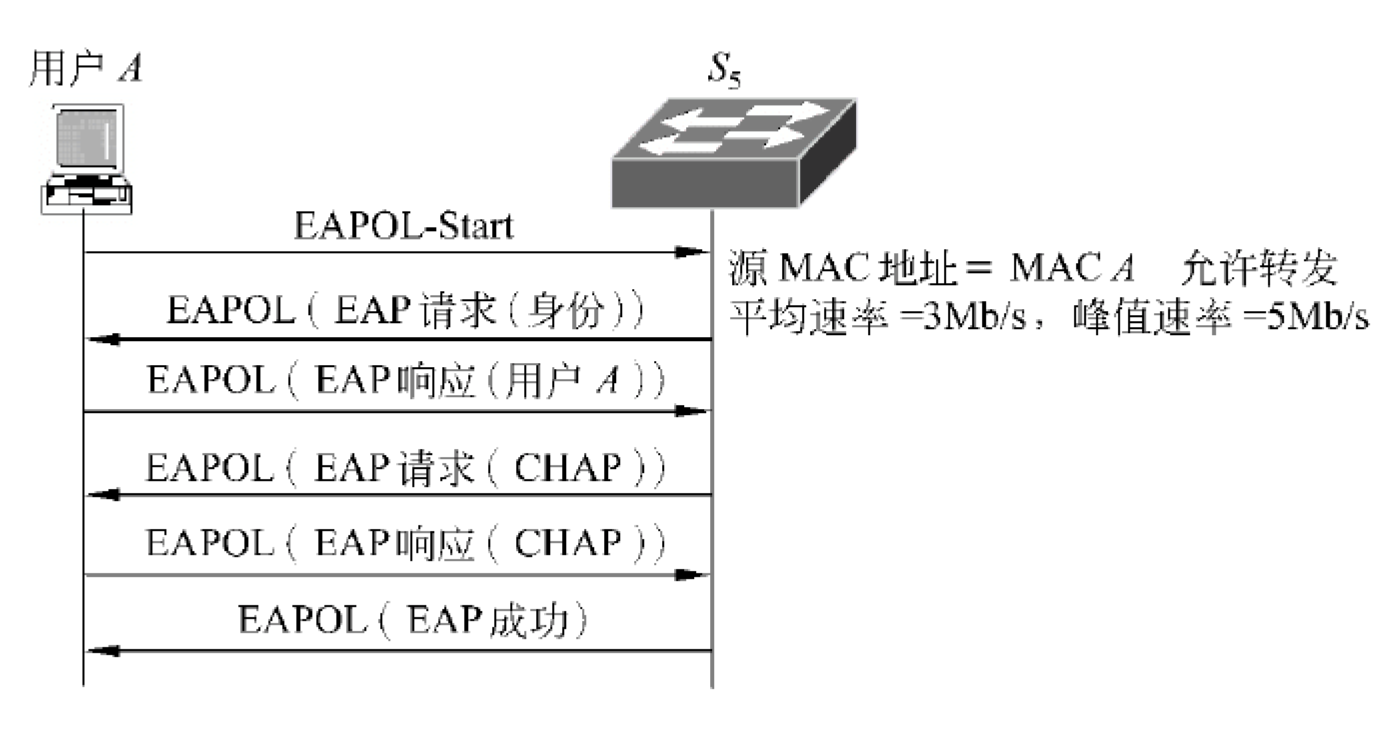


图 10.2　认证用户身份过程

2．防火墙访问控制机制

1）配置防火墙访问控制策略

防火墙端口 1、2 和 3 分别绑定内部网络（信任区）、非军事区和外部网络（非信任区），内部网络分配给用户终端的子网地址范围是 200.1.0.0/24～200.1.7.0/24，图 10.2 中

只给出了分配 200.1.1.0/24～200.1.5.0/24 范围子网地址的用户终端，根据制定的网络安全策略，对防火墙配置如下访问控制策略：

(1) 从信任区到非军事区 源 IP 地址＝200.1.0.0/21 目的 IP 地址＝193.1.2.5/32 HTTP 服务；

(2) 从信任区到非军事区 源 IP 地址＝200.1.0.0/21 目的 IP 地址＝193.1.2.6/32 SMTP＋POP3 服务；

(3) 从信任区到非信任区 源 IP 地址＝200.1.0.0/21 目的 IP 地址＝0.0.0.0 HTTP＋FTP GET 服务；

(4) 从非军事区到非信任区 源 IP 地址＝193.1.2.6/32 目的 IP 地址＝0.0.0.0 SMTP 服务；

(5) 从非信任区到非军事区 源 IP 地址＝0.0.0.0 目的 IP 地址＝193.1.2.5/32 HTTP GET 服务；

(6) 从非信任区到非军事区 源 IP 地址＝0.0.0.0 目的 IP 地址＝193.1.2.6/32 SMTP 服务；

(7) 从非信任区到信任区 第 2 层隧道 源 IP 地址＝200.1.11.0/24 目的 IP 地址＝200.1.9.5/32 FTP 服务。

2) 内部网络终端访问外部网络资源过程

某个内部网络终端通过浏览器访问外部网络中的某个 Web 服务器的信息交换过程如图 10.3 所示，当防火墙通过端口 1 接收到封装 TCP 报文的 IP 分组，首先在会话表中查找对应项，用于检索会话表的信息有源和目的 IP 地址、源和目的端口号，如果在会话表中找到对应项，则通过会话表给出的信息直接转发，否则，通过检索路由表得到转发端口：端口 3。在获取输入区(端口 1 绑定的信任区)和输出区(端口 3 绑定的非信任区)后，匹配访问控制策略，这里，和访问控制策略(3)匹配：从信任区输入；从非信任区输出；源 IP 地址属于内部网络终端地址范围 200.1.0.0/21；目的 TCP 端口号＝80，表明是 HTTP 服

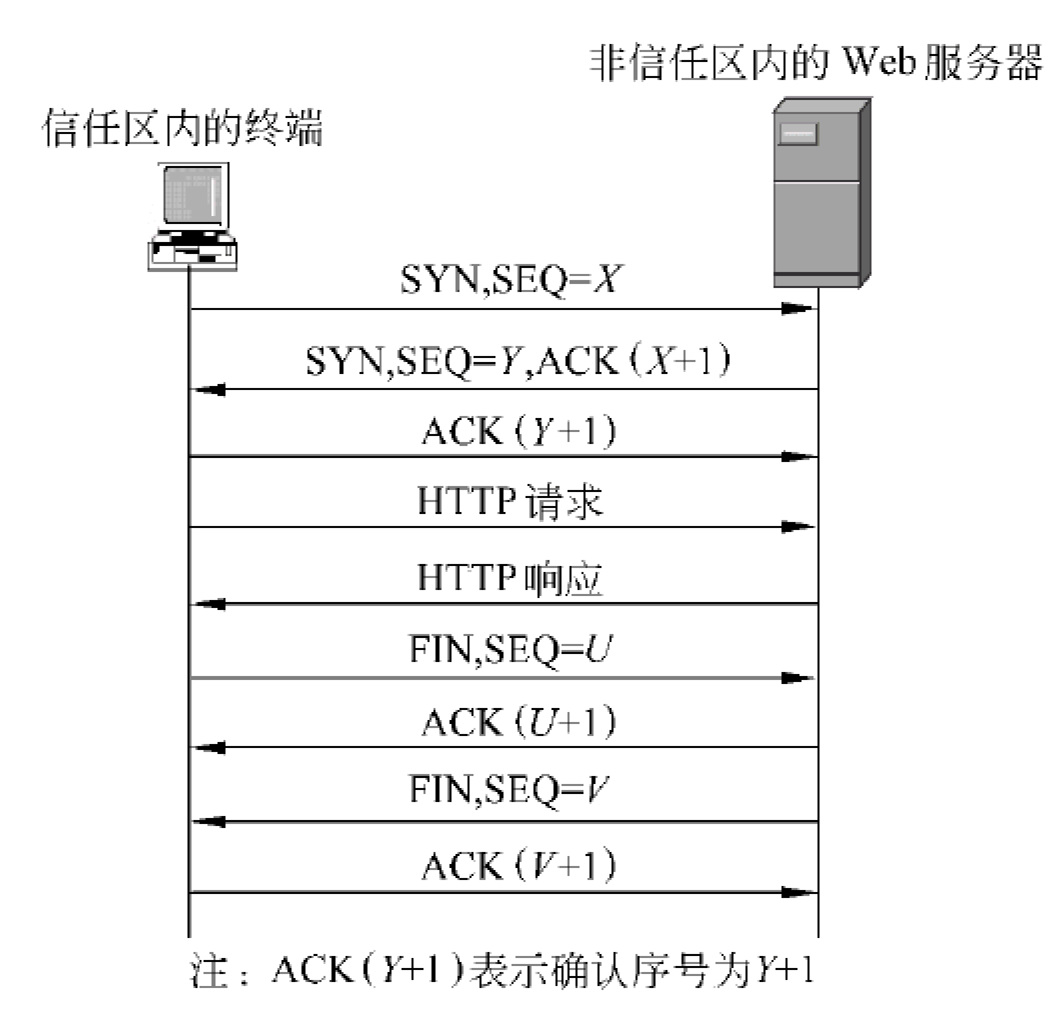


图 10.3 HTTP 服务信息交换过程

务。因此,允许该服务过程继续。由于防火墙端口 1 设置为 NAT 工作方式,在通过端口 3 输出该 IP 分组前,需要完成本地 IP 地址至全球 IP 地址的转换过程。假定防火墙端口 1 配置的全球 IP 地址池为 193.1.1.1～193.1.1.254,防火墙端口 1 将从全球 IP 地址池中选择一个未分配的全球 IP 地址作为该内部网络终端访问外部网络中 Web 服务器所使用的全球 IP 地址。在完成 TCP 连接建立过程后,会话表中产生表 10.2 所示的一项。

表 10.2　会话表

源 IP 地址	源端口号	目的 IP 地址	目的端口号	全球 IP 地址	支持服务	输入端口	输出端口	状　态
200.1.1.1	1234	12.13.4.5	80	193.1.1.1.	HTTP	端口 1	端口 3	建立连接
			⋮					

表 10.2 中的该项内容表明从端口 1 接收到的源 IP 地址＝200.1.1.1、目的 IP 地址＝12.13.4.5、源端口号＝1234、目的端口号＝80 的 IP 分组,将从端口 3 转发出去,并且在转发出去前将源 IP 地址替换成全球 IP 地址 193.1.1.1。反之,从端口 3 接收到的源 IP 地址＝12.13.4.5、目的 IP 地址＝193.1.1.1、源端口号＝80、目的端口号＝1234 的 IP 分组,将从端口 1 转发出去,并且在转发出去前将源 IP 地址替换成内部 IP 地址 200.1.1.1。正常情况下,会话表中该项内容在释放内部网络终端和外部网络中 Web 服务器之间的 TCP 连接后删除,同时将全球 IP 地址 193.1.1.1 归还给全球 IP 地址池。

3）VPN 接入过程

VPN 接入过程如图 10.4 所示,内部员工终端作为接入终端通过建立动态连接的方式和防火墙建立连接,并由防火墙完成身份认证和内部网络本地 IP 地址分配,接入终端用点对点协议(PPP)实现动态连接建立过程,PPP 是一种基于点对点链路的链路层协议,而接入终端和防火墙之间并不是点对点链路,而是 Internet,因此,必须建立基于 Internet 的虚拟点对点链路,即用于传输 PPP 帧的第 2 层隧道,隧道两端分别是接入终端和防火墙,第 2 层隧道报文是以隧道两端全球 IP 地址为源和目的 IP 地址的 IP 分组。

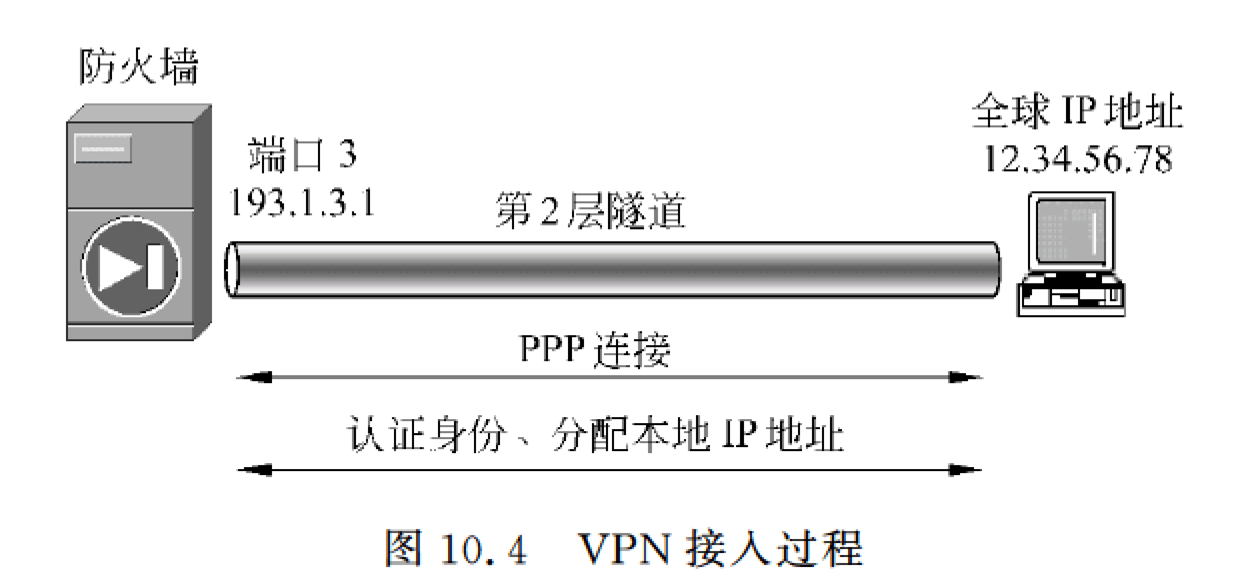


图 10.4　VPN 接入过程

为了传输安全,经过第 2 层隧道传输的 IP 分组必须采用 IPSec 协议进行发送端认证和数据加密,因此,需要在隧道两端之间建立双向的安全关联(SA),由于安全关联是动态生成的,因此,需要采用 Internet 安全关联和密钥管理协议(Internet Security Association and key Management Protocol,ISAMP)动态建立隧道两端的双向安全关联。

由此可以得出需要分两部分完成对防火墙端口 3 的配置,第一部分是有关第 2 层隧

道和安全关联的配置，第二部分是有关 PPP 的配置，有关第 2 层隧道和安全关联的配置主要完成隧道两端参数、IPSec 使用的认证和加密算法、密钥生成机制等设置，有关 PPP 的配置主要完成可供分配的内部网络地址池、接入用户名和口令、认证接入用户的认证协议等设置。

第 2 层隧道相关配置：

- 接入用户标识符：用户 A。
- 隧道本地接口和 IP 地址：端口 3，193.1.3.1。
- 隧道远端 IP 地址：任意。

安全关联第 1 阶段配置：

- 加密算法：DES。
- D-H 组号：2。
- 认证机制：数字签名。
- 完整性检测算法：数字签名。

安全关联第 2 阶段配置：

- 安全协议：ESP。
- 加密算法：AES。
- D-H 组号：2。
- 认证算法：HMAC-MD5-96。
- 模式：运输。

PPP 配置：

- 内部网络本地 IP 地址池：200.1.11.1～200.1.11.254。
- 用户名：用户 A。
- 口令：PASSA。
- 认证协议：CHAP。

由于接入终端的全球 IP 地址不是固定的，因此，在配置隧道两端参数时，可以不指定接入终端一端的全球 IP 地址，但在实际建立隧道两端之间的安全关联时，接入终端必须已经分配全球 IP 地址。

如果采用安全传输机制，首先需要建立隧道两端之间的安全关联，建立安全关联的第一步是完成隧道两端之间的身份认证，在这里由内部网络的认证中心统一为防火墙和需要远程接入内部网络的员工签发证书，证书中将用户名和分配给该用户的公钥绑定在一起，证书由内部网络认证中心的私钥加密，而内部网络认证中心的公钥是公开的。因此，首先在防火墙配置允许远程接入的内部员工的用户名列表，只有当接收到的证书中给出的用户名包含在允许远程接入的内部员工的用户名列表中，且该证书的真实性通过认证中心公钥确认，才继续通过测试该用户是否拥有证书中公钥所对应的私钥来确定接入用户身份。

建立安全关联需要进行两个阶段，每一个阶段都需要配置相关参数。一旦隧道两端成功建立安全关联，防火墙和远程接入终端各自建立如表 10.3 和表 10.4 所示的安全关联表。

表 10.3　防火墙安全关联表

输出	源 IP 地址＝192.1.3.1/32 • AND • 目的 IP 地址＝12.34.56.78/32					
	SPI	安全协议	加密算法	认证算法	加密密钥	认证密钥
	12345678H	ESP	AES	HMAC-MD5-96	K_{11}	K_{12}
输入	目的 IP 地址＝193.1.3.1/32 • AND • SPI＝87654321H • AND • 安全协议＝ESP					
	SPI	安全协议	加密算法	认证算法	加密密钥	认证密钥
	87654321H	ESP	AES	HMAC-MD5-96	K_{21}	K_{22}

表 10.4　远程接入终端安全关联表

输出	源 IP 地址＝12.34.56.78/32 • AND • 目的 IP 地址＝192.1.3.1/32					
	SPI	安全协议	加密算法	认证算法	加密密钥	认证密钥
	87654321H	ESP	AES	HMAC-MD5-96	K_{21}	K_{22}
输入	目的 IP 地址＝12.34.56.78/32 • AND • SPI＝12345678H • AND • 安全协议＝ESP					
	SPI	安全协议	加密算法	认证算法	加密密钥	认证密钥
	12345678H	ESP	AES	HMAC-MD5-96	K_{11}	K_{12}

在建立隧道两端之间的双向安全关联后，接入终端首先建立基于 Internet 的虚拟点对点链路——第 2 层隧道，在完成第 2 层隧道建立后，接入终端用 PPP 完成接入过程，首先用 PPP LCP 建立 PPP 链路，建立 PPP 链路的目的是协调接入终端和防火墙之间和后续接入操作有关的参数，如 PPP 帧封装格式、采用的认证协议等，在完成 PPP 链路建立后，根据建立 PPP 链路时指定的认证协议完成接入用户的身份认证，这里，防火墙采用 CHAP 作为接入用户身份认证协议，并在防火墙 PPP 配置中给出接入用户名和对应的口令。只有当防火墙通过 CHAP 确认接入终端的用户名＝用户 A 且口令＝PASSA 时，才通过 IPCP 为接入终端分配内部网络本地 IP 地址，这里假定防火墙在内部网络本地 IP 地址池中选择 200.1.11.1 作为分配给接入终端的内部网络本地 IP 地址。整个接入过程如图 10.5 所示。

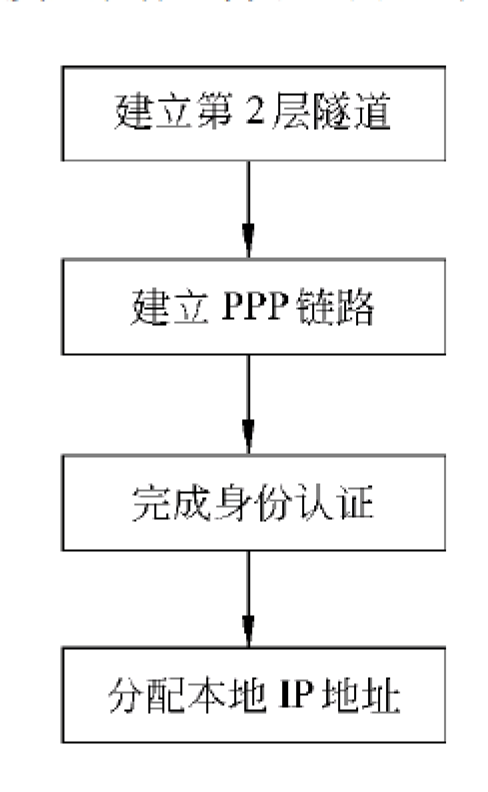


图 10.5　接入操作过程

接入终端完成接入过程中和防火墙之间传输的数据，均需封装成 PPP 帧格式，但 PPP 帧并不直接在点对点链路上传输，而是通过基于 Internet 的第 2 层隧道进行传输，因此，PPP 帧又需要封装成第 2 层隧道（L2TP）格式，由于第 2 层隧道是基于 Internet，因此，最终需要封装成以接入终端和防火墙端口 3 全球 IP 地址为源和目的 IP 地址的 IP 分组，即第 2 层隧道报文，如果不采用 IPSec，第 2 层隧道格式既可以先封装成 UDP 报文，然后封装成 IP 分组，也可以直接封装成 IP 分组；如果采用 IPSec，则需先将第 2 层隧道格式封装成 UDP 报文，然后

再封装成 IP 分组，封装过程如图 10.6 所示。

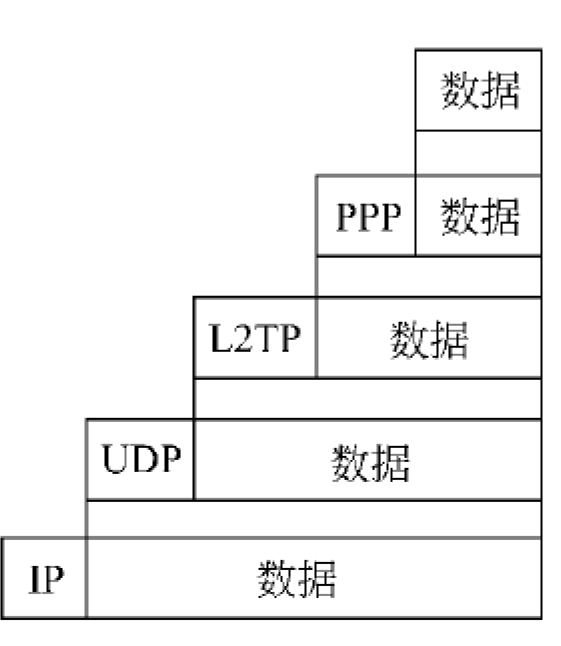


图 10.6 数据封装过程

接入终端接入内部网络后，建立图 10.7 所示的接入终端和内部网络中 FTP 服务器之间的传输通路，防火墙作为路由器，一端通过端口 1 连接的以太网和内部网络中的 FTP 服务器相连，另一端通过端口 3 连接的第 2 层隧道和接入终端相连，由于接入终端用虚拟点对点链路(第 2 层隧道)连接第一跳路由器——防火墙，因此，所有传输给内部网络中 FTP 服务器的数据首先通过第 2 层隧道传输给防火墙，经防火墙转发后，传输给内部网络中的 FTP 服务器。图 10.8 给出接入终端封装传输给防火墙的数据的过程，其中 IP 分组首部中协议字段值 50 表明 IP 分组净荷是 ESP 报文，ESP 首部中下一个首部字段值 17 表明 ESP 报文净荷是 UDP 报文，UDP 报文目的端口号 1701 表明 UDP 报文净荷是第 2 层隧道格式。

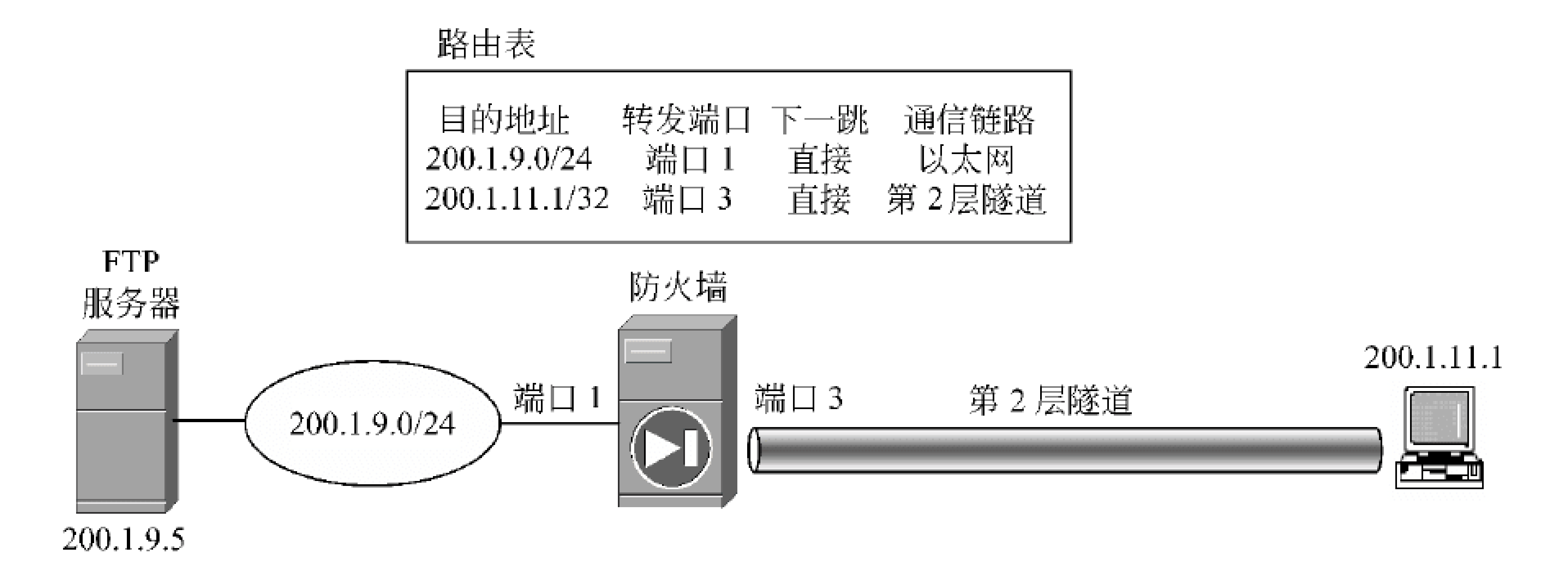


图 10.7 接入终端和内部网络 FTP 服务器之间传输通路

3. 入侵防御系统监测攻击机制

1）主机入侵防御系统

数据库服务器中的主机入侵防御系统主要实现下述功能：

- 服务器安全状态监测：服务器安全状态包括主机防火墙配置、打开的服务类型、病毒入侵情况、操作系统和数据库应用系统存在的漏洞及对应补丁软件下载、运行情况。
- 网络信息流检测：对从网卡接收到的信息流进行检测，确定是否符合应用层协议要求的请求/响应方式，是否符合数据库访问规范，是否符合 TCP 操作规范，各个字段值是否符合协议要求格式和取值范围。
- 服务器资源访问控制：限制对服务器资源的访问，如禁止远程用户修改注册表等系统信息资源。
- 进程调度控制：禁止网络应用进程调用命令解释程序或安装程序。

2）网络入侵防御系统

- 监测异常信息流：分别在 IP 层、运输层、应用层监测传输给数据库服务器的信息

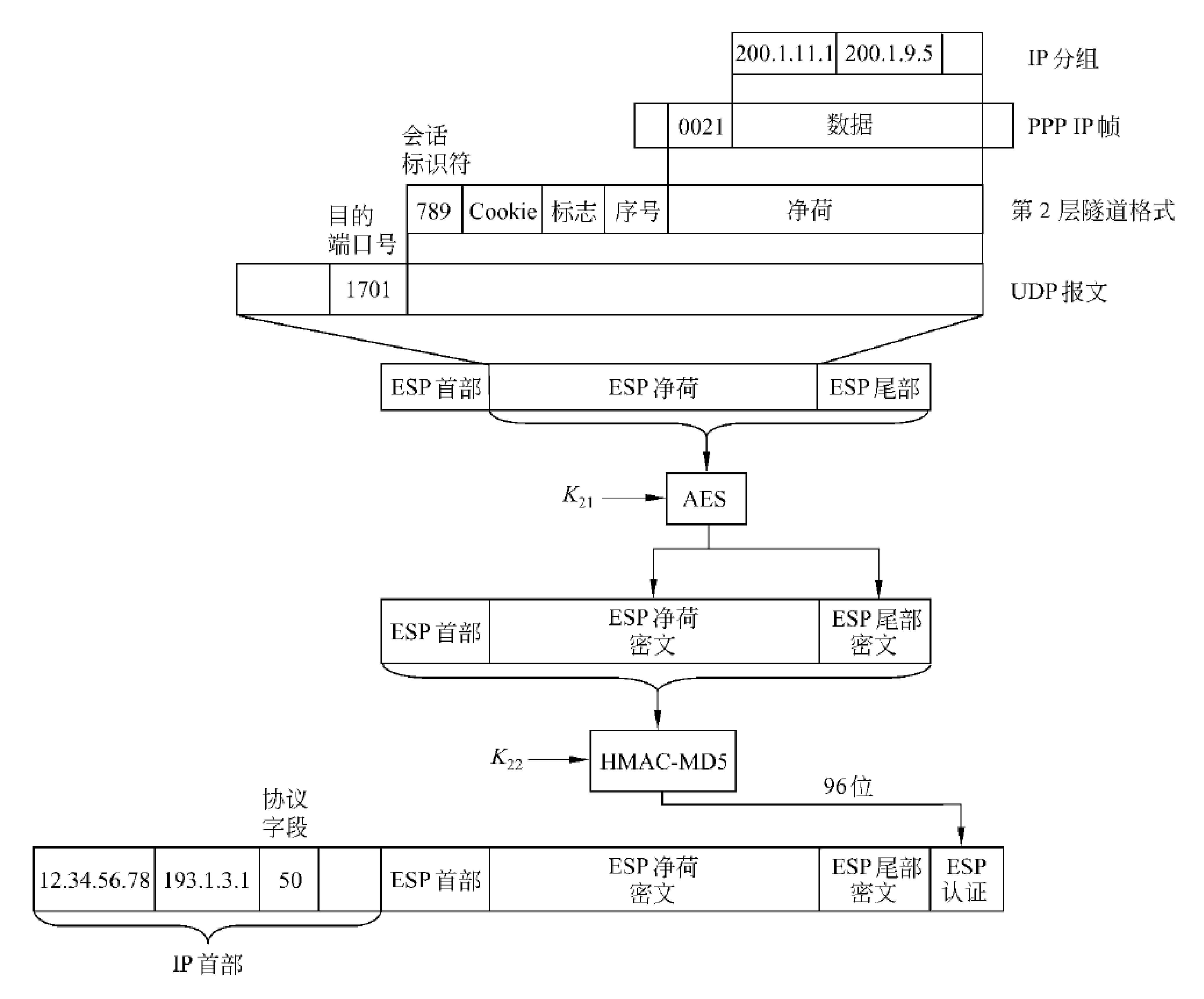


图 10.8　接入终端封装数据过程

流，一旦监测到不符合 IP 要求的 IP 分组，如包含不合理字段值、分片后的净荷长度总和超过 64KB 等；不符合运输层要求的 TCP 或 UDP 报文，如标志位不统一、序号重叠等；不符合应用层协议要求的请求/响应报文，如字段取值超出协议允许范围、响应报文内容和请求报文内容不存在逻辑关联等，登记源 IP 地址，释放用于传输信息流的 TCP 连接，并向安全管理员报告。

- 监测攻击特征：针对数据库应用系统特点，定义攻击特征库，对传输给数据库服务器的信息流实施监测，不允许包含攻击特征库中任何攻击特征的信息流传输给数据库服务器。
- 监测拒绝服务攻击：监测是否发生 SYN 泛洪、定向广播等拒绝服务攻击，隔断这些攻击对数据库服务器的影响。
- 监测端口扫描：监测是否发生针对数据库服务器的端口扫描，一旦发现，及时终止侦察过程，登记源 IP 地址，并向安全管理员报告。
- 监测交互式信息流：监测是否存在具有交互特性的信息流模式，一旦发现，及时释放相关 TCP 连接，登记源 IP 地址，并向安全管理员报告。

第11章 应用层安全协议

CHAPTER

11.1 Web 安全协议

11.1.1 Web 安全问题

Web 安全的重要性在于一是 Web 网站已经成为电子商务和网络银行平台，用户通过 Web 网站实现网络购物和电子转账等商务活动，二是由于通过浏览器访问网络资源的方便性，大量数据库应用系统采用 B/S 结构，即统一用浏览器作为用户访问数据库服务器的客户端软件，企业网络应用系统也常常将 Web 网站作为访问企业网络资源的入口。正因为如此，大量的攻击也针对 Web 网站展开。

- 伪造和篡改 Web 主页：伪造著名网站主页，并用该著名网站相似的域名注册，以此诱使用户登录、访问，如伪造某个银行的网页，采用和该银行域名相似的域名注册该网页，诱使用户登录该伪造网页进行电子转账活动，以此套取用户账号和密码。有的黑客在攻击某个网站后，在该网站网页上用著名网站域名链接伪造网页，诱使用户访问伪造网页。
- 截取用户私密信息：通过拦截用户传输给某个商务网站的信息获取用户私密信息。
- 拒绝服务攻击：通过消耗服务器资源和连接服务器的网络资源，如服务器 TCP 会话表、服务器内存、服务器硬盘空间、网络中路由器的处理能力、网络连接服务器链路的带宽等，使服务器丧失通信能力和服务能力。

11.1.2 Web 安全机制

彻底解决 Web 网站所面临的安全威胁需要构建网络安全体系，这里讨论的 Web 安全机制主要着重于解决用户端和服务器端之间的相互认证和信息的保密传输问题。

网络体系结构中的多层均有实现端到端的相互认证和保密传输的机制，如图11.1所示。在网络层用IPSec协议实现端到端的相互认证和保

密传输，如图 11.1(a)所示，由于这种安全机制对运输层是透明的，通用性更好。在 TCP 上用运输层安全(Transport Layer Security，TLS)协议实现端到端的相互认证和保密传输，如图 11.1(b)所示，由于 TLS 对应用层协议是透明的，多种应用层协议均可通过 TLS 实现端到端的相互认证和保密传输，也有较好的通用性。安全电子交易(Secure Electronic Transaction，SET)协议是实现网络安全电子交易的协议，如图 11.1(c)所示，由于具有针对性，因此能够更有效地解决网络电子交易所面临的安全问题。IPSec 认证和保密传输机制已在前面章节中充分讨论，这里主要讨论 HTTP over TLS(HTTPS)和 SET 这两种 Web 安全机制。

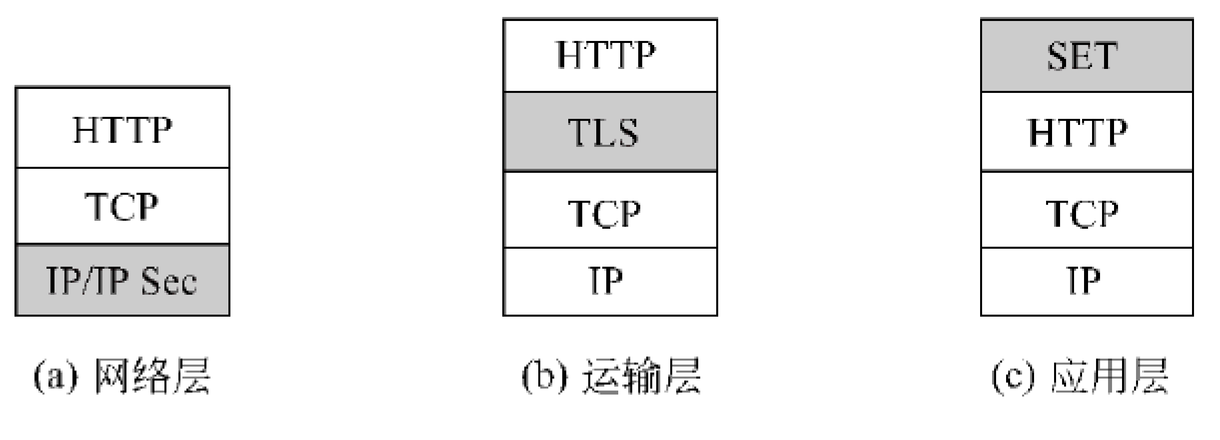


图 11.1 Web 安全机制

11.1.3 HTTP over TLS

HTTP over TLS (HTTPS)的 Web 安全机制体现在两方面：服务器身份认证与终端和服务器之间保密传输，整个操作过程如图 11.2 所示。

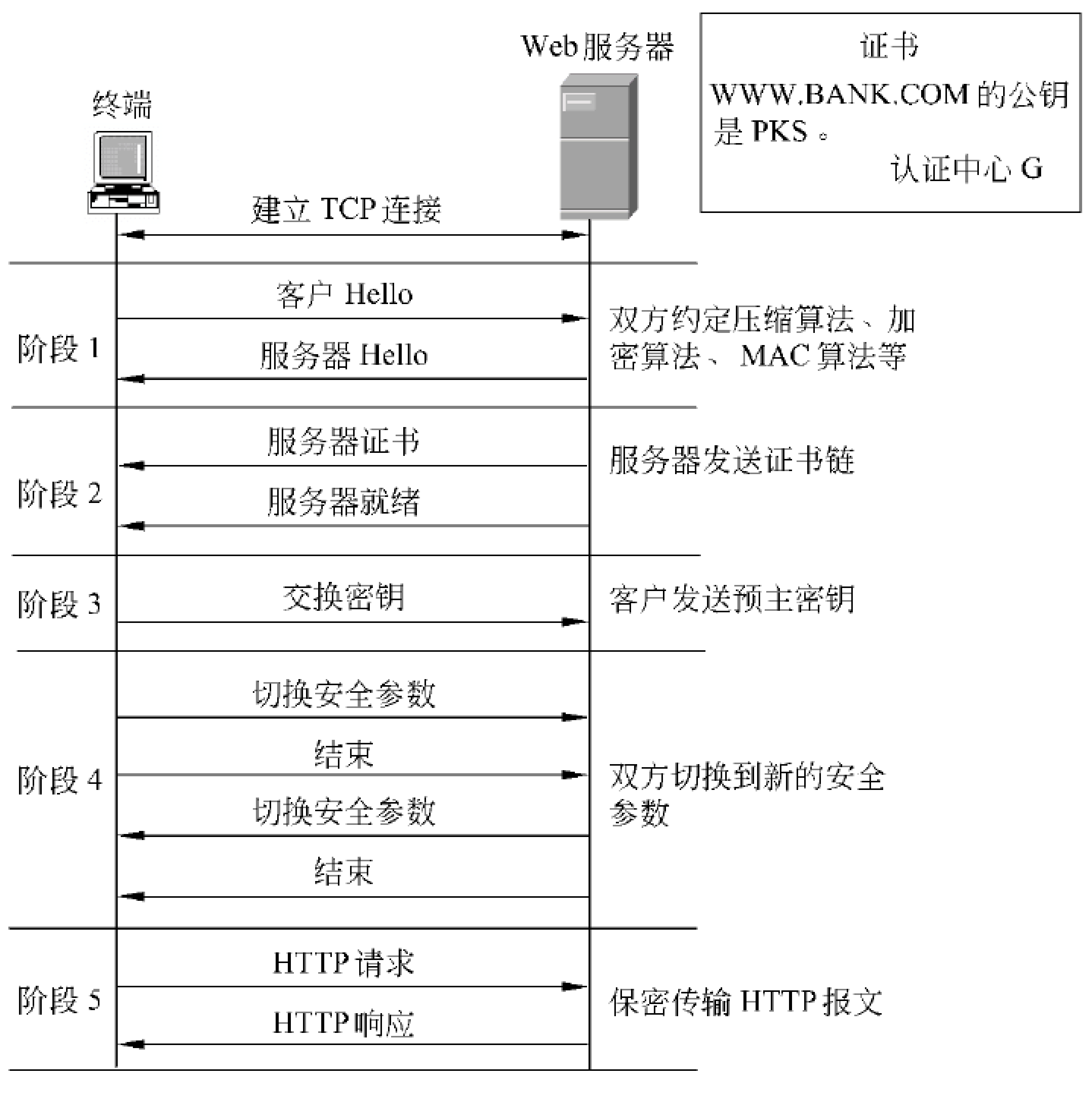


图 11.2 HTTPS 操作过程

1．服务器身份认证

为了防止访问伪造的网站，在信息交换之前必须认证 Web 服务器的身份，假定图 11.2 中的 Web 服务器是 URL＝WWW.BANK.COM 的网站，Web 服务器在提供服务前需要获得某个权威认证中心签发的证书，证书证明 URL＝WWW.BANK.COM 和公钥 PKS 的绑定关系。终端和服务器首先通过交换客户 Hello 和服务器 Hello 消息，选定传输 HTTP 报文时使用的压缩算法、加密算法、认证算法，然后由服务器向终端发送证书链，如果签发服务器证书的认证中心链如图 11.3 所示，则服务器发送的证书链为 *A*＜＜*C*＞＞、*C*＜＜*G*＞＞、*G*＜＜WWW.BANK.COM＞＞，即由认证中心 *A* 签发的证明认证中心 *C* 和公钥 PKC 绑定关系的证书，认证中心 *C* 签发的证明认证中心 *G* 和公钥 PKG 绑定关系的证书，认证中心 *G* 签发的证明 URL＝WWW.BANK.COM 的网站和公钥 PKS 绑定关系的证书。假定终端已经证实认证中心 *C* 的公钥 PKC，则可用 PKC 证实认证中心 *G* 和公钥 PKG 的绑定关系，又用 PKG 证实 URL＝WWW.BANK.COM 的网站和公钥 PKS 的绑定关系。在证实了 URL＝WWW.BANK.COM 的网站和公钥 PKS 的绑定关系后，只要确定服务器拥有公钥 PKS 对应的私钥 SKS，即可证实服务器就是 URL＝WWW.BANK.COM 的网站。

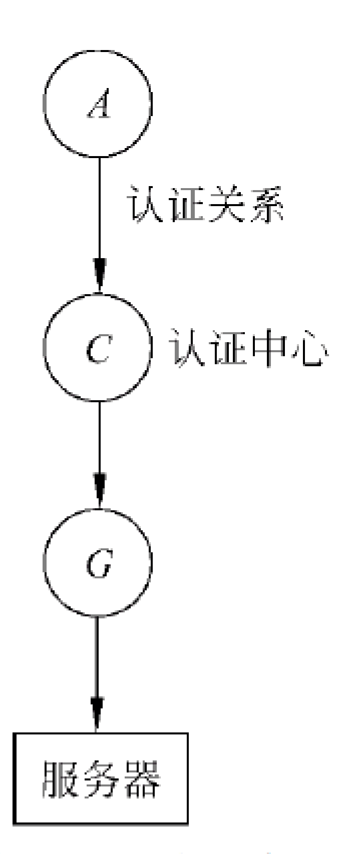


图 11.3　认证中心链

为了证实服务器拥有公钥 PKS 对应的私钥 SKS，终端通过密钥交换消息向服务器发送 E_{PKS}(PMK)，PMK 是 48B 长度的预主密钥，由终端随机产生，*E* 是 RSA 加密算法。终端然后根据 PMK 计算出主密钥 MK＝PRF(PMK，"master secret"，NonceC ‖ NonceS)，NonceC 和 NonceS 是分别由客户和服务器随机产生的随机数，通过客户 Hello 和服务器 Hello 消息告知对方。服务器通过解密运算后获得预主密钥 PMK＝D_{SKS}(E_{PKS}(PMK))(*D* 是 RSA 解密算法)，用和终端同样的方法计算出主密钥 MK，然后在发送给终端的结束消息中包含 PRF(MK，"server finished"，MD5(握手协议消息) ‖ SHA-1(握手协议消息))计算结果，终端用自己的主密钥同样计算出 PRF(MK，"server finished"，MD5(握手协议消息) ‖ SHA-1(握手协议消息))，并将其和服务器结束消息中包含的计算结果比较，如果相等，意味着终端和服务器拥有相同的主密钥，由于主密钥由预主密钥计算所得，而正确解密预主密钥需要拥有公钥 PKS 对应的私钥 SKS，以此证实服务器的身份，否则，认证服务器失败，终止 HTTPS 操作过程。

2．计算加密和认证密钥

为了保证终端和服务器之间数据传输的保密性和完整性，一是必须在传输的数据中插入用于检测数据完整性的消息认证码(MAC)，可供选择的计算 MAC 的算法有 HMAC-MD5-128 或 HMAC-SHA-1-160，无论选择 HMAC-MD5-128 或 HMAC-SHA-1-160 计算 MAC，均需认证密钥。二是必须对数据进行加密，TLS 支持的加密算法如表 11.1 所示，终端和服务器通过交换客户 Hello 和服务器 Hello 消息，选定加密算法，一旦选定加密算法，需要对应长度的加密密钥，如 3DES 需要 168 位的加密密钥。服务器和终端可以采用不同的认证密钥和加密密钥，但它们均通过主密钥 MK 计算所得。

表 11.1　TLS 支持的加密算法及密钥长度

分组密码体制		流密码体制	
算　　法	密钥长度/B	算　　法	密钥长度/B
IDEA	128	RC4-40	40
RC2-40	40	RC4-128	128
DES-40	40		
DES	56		
3DES	168		

公式 PRF(MK,“key expansion”,NonceC ‖ NonceS)的计算结果长度是可变的,取决于 P_MD5 和P_SHA-1 的重复计算次数(参见 3.4.2 节),因此,通过适当选择 P_MD5 和 P_SHA-1 的重复计算次数,可以使得公式 PRF(MK,“key expansion”,NonceC ‖ NonceS)的输出结果长度为(2×24+2×20+2×8)B=108B。在选择 3DES 作为加密算法,HMAC-SHA-1-160 作为计算 MAC 的算法,且终端和服务器采用不同的加密密钥、认证密钥和初始向量的前提下,其中终端和服务器的加密密钥长度各为 24B(每个字节的最高位不用,24×7=168 位 3DES 加密密钥),认证密钥长度各为 20B,初始向量长度各为 8B。

3. HTTP 报文传输过程

建立 TLS 连接后,终端和服务器约定下述参数:

- 加密算法:3DES。
- 计算 MAC 算法:HMAC-SHA-1-160。
- 终端认证密钥:K_1(20B)。
- 终端加密密钥:K_{11}、K_{12}、K_{13}(3×8B,其中最高位不用)。
- 服务器认证密钥:K_2(20B)。
- 服务器加密密钥:K_{21}、K_{22}、K_{23}(3×8B,其中最高位不用)。
- 终端初始向量:IV1。
- 服务器初始向量:IV2。
- 发送序号:0。
- 接收序号:0。

如果采用压缩算法,还需约定压缩算法类型、版本。终端经过 TLS 连接发送 HTTP 报文的过程如图 11.4 所示。HTTP 报文首先分段,分段的目的是使其长度适合 TLS 记录协议的净荷长度,如果采用压缩算法,用压缩算法将分段后的数据压缩,压缩后的数据和压缩算法类型、版本、压缩后数据长度、发送序号串接在一起,进行 HMAC-SHA-1-160 运算,得到 160 位的 MAC,MAC 添加在压缩后数据尾部,构成需要传输的明文,再对明文进行 3DES 加密运算(图中用 3DESE 表示),产生密文,密文作为 TLS 记录协议报文的净荷,加上 TLS 记录协议首部,构成 TLS 记录报文,经过 TLS 连接传输给服务器,服务器通过如图 11.4 所示的操作过程的逆操作确定数据的完整性,并最终还原 HTTP 报文。终端和服务器的初始发送、接收序号为 0,每发送一个 TLS 记录协议报文,发送序号增 1,

每接收一个 TLS 记录协议报文，接收序号增 1，接收端重新计算 MAC 时，用接收序号串接解密后得到的压缩数据及压缩算法类型、版本、压缩后数据长度，并对串接结果进行 HMAC-SHA-1-160 运算，如果运算结果和 TLS 记录协议报文中的 MAC 不同，表明数据完整性检测失败。序号参与 MAC 计算的目的是使接收端能够检测出重复传输的 TLS 记录协议报文，以此防止中继攻击(亦称重放攻击)，当然，该机制也可检测出传输过程中发生 TLS 记录协议报文丢弃的情况。

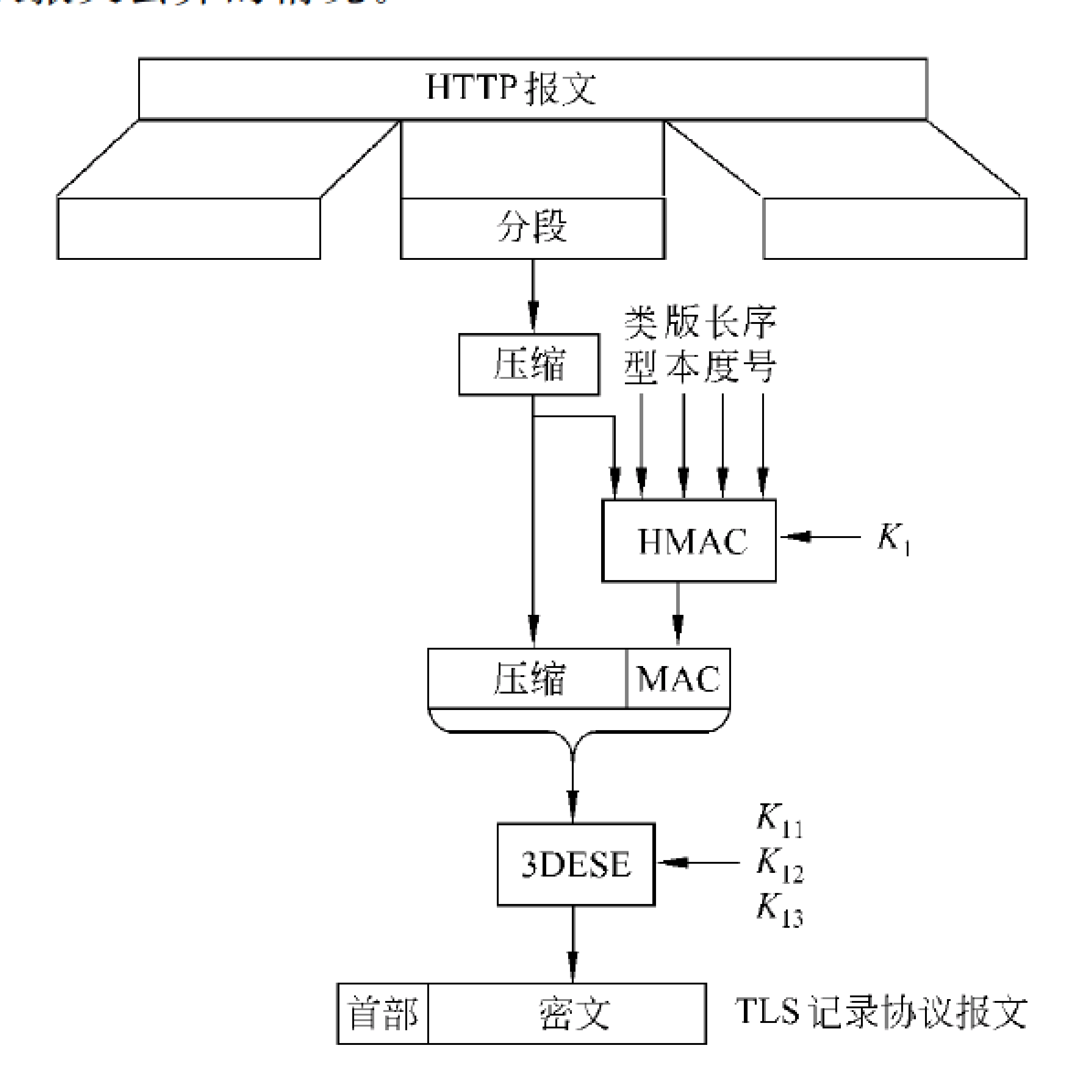


图 11.4　终端发送 HTTP 报文过程

11.1.4　SET

1. SET 应用系统

安全电子交易(Secure Electronic Transaction，SET)用于保证基于 Internet 的信用卡交易的安全进行，其应用系统如图 11.5 所示，由持卡人、商家、支付网关、认证中心链、发卡机构、商家结算机构组成。支付网络是互联发卡机构、商家结算机构等金融机构，并完成资金电子转账的专用网络，持卡人、商家和支付网关通过交换、处理 SET 消息完成电子交易，支付网关、发卡机构和结算机构之间通过专用的支付系统实现资金电子转账。

- 持卡人：拥有正规发卡机构发行的信用卡或其他支付卡，通过连接 Internet 的个人计算机(PC)在网络上完成向商家购物的个人或集体。
- 商家：通过 Internet 向持卡人提供商品或服务的个人或集体，允许持卡人通过信用卡或其他支付卡结算货款，但持卡人拥有的信用卡或其他支付卡必须是商家结算机构认可的。
- 发卡机构：负责向持卡人发卡，并开设账户的金融机构，如银行，同时，负责向商家支付持卡人用卡消费的金额。
- 商家结算机构：负责为商家建立账户，认证持卡人用于消费的信用卡或支付卡的有效性，通过和发卡机构协调完成货款支付的金融结构。商家通常需要支持由多

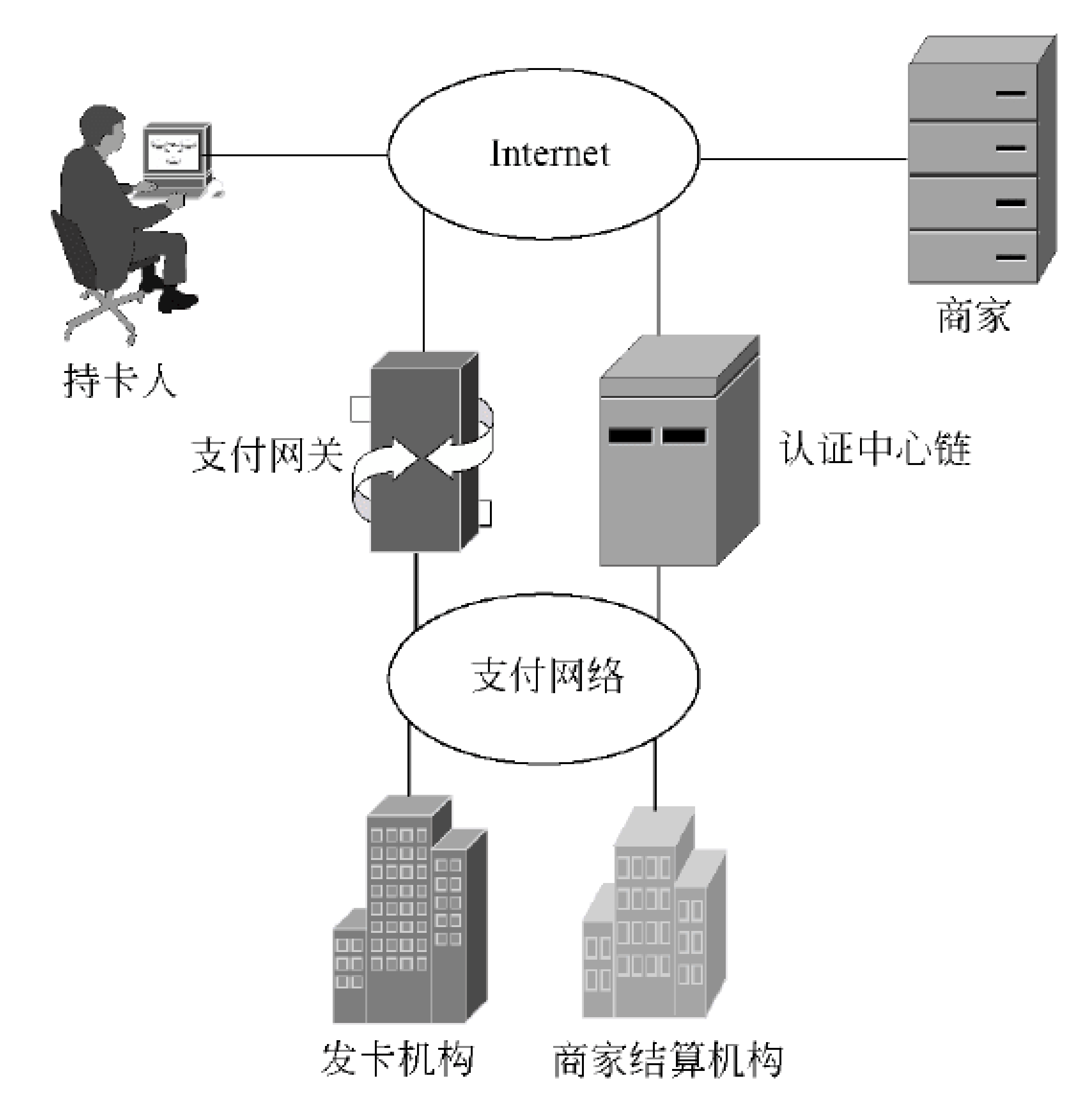


图 11.5 SET 应用系统

种不同发卡结构发行的信用卡,但出于运行成本的考虑,不愿意和多家发卡结构直接建立结算关系,而是统一委托给某个中介结算机构,由该结算机构负责认证信用卡账户的有效性,消费金额是否超过该信用卡的信用额度,并通过支付网络完成资金从发卡机构到商家账户之间的电子转账。

• 支付网关:一是实现 Internet 和支付网络之间的互联,二是实现 SET 消息和金融机构支付系统实现电子转账所要求的消息之间的相互转换,商家通过 Internet 和支付网关交换用于认证信用卡有效性、获取信用卡信用额度的 SET 消息,支付网关根据 SET 消息内容,通过支付网络和金融机构交换支付系统所支持的命令和响应消息。
• 认证中心:是持卡人、商家、支付网关、金融机构都信任的证书签发机构,签发证明持卡人和信用卡账户之间绑定关系,商家、支付网关和金融机构身份的证书。

2. SET 目标

• 保证订货和支付信息的保密性:通过加密保证只有合法的接收者才能读取信息,同时减少冒充持卡人进行电子交易的风险。
• 保证数据的完整性:通过报文摘要算法和数字签名技术保证经过网络传输的数据的完整性,确保电子交易过程所涉及的 SET 消息是未被篡改的。
• 认证持卡人和信用卡之间的绑定关系:发卡机构发行信用卡后,必须开设相应账户,认证持卡人和信用卡之间的绑定关系就是确认持卡人是该账户的合法拥有者。数字签名技术和证书是认证持卡人是某个账户的合法拥有者的主要机制。
• 认证商家身份:通过数字签名技术和证书确认商家身份,并确认和商家进行的电子交易是安全的。
• 确保合法参与电子交易的各方的安全:加密、认证机制保证合法参与电子交易的

各方的安全。

- 电子交易安全与运输层无关：电子交易的安全性独立于所使用的运输层协议，无须运输层提供类似 TLS 这样的安全传输协议就能实现电子交易的安全性。
- SET 应用系统独立于传输网络和主机操作系统平台：SET 协议和报文格式独立于传输 SET 消息的传输网络，处理 SET 消息的硬件平台和操作系统。

3. 加密和认证机制

对于如图 11.6 所示的认证中心链，持卡人、商家和支付网关必须得到认证中心签发的证书，同时，每一方必须具有其他各方的证书和确认证书有效性的证书链：

持卡人

$A<<C>>$，$C<<F>>$，$F<<$商家 $A>>$

$A<<D>>$，$D<<G>>$，$G<<$支付网关 $G>>$

商家

$A<<B>>$，$B<<E>>$，$E<<$账户 $C>>$

$A<<D>>$，$D<<G>>$，$G<<$支付网关 $G>>$

支付网关

$A<<B>>$，$B<<E>>$，$E<<$账户 $C>>$

$A<<C>>$，$C<<F>>$，$F<<$商家 $A>>$

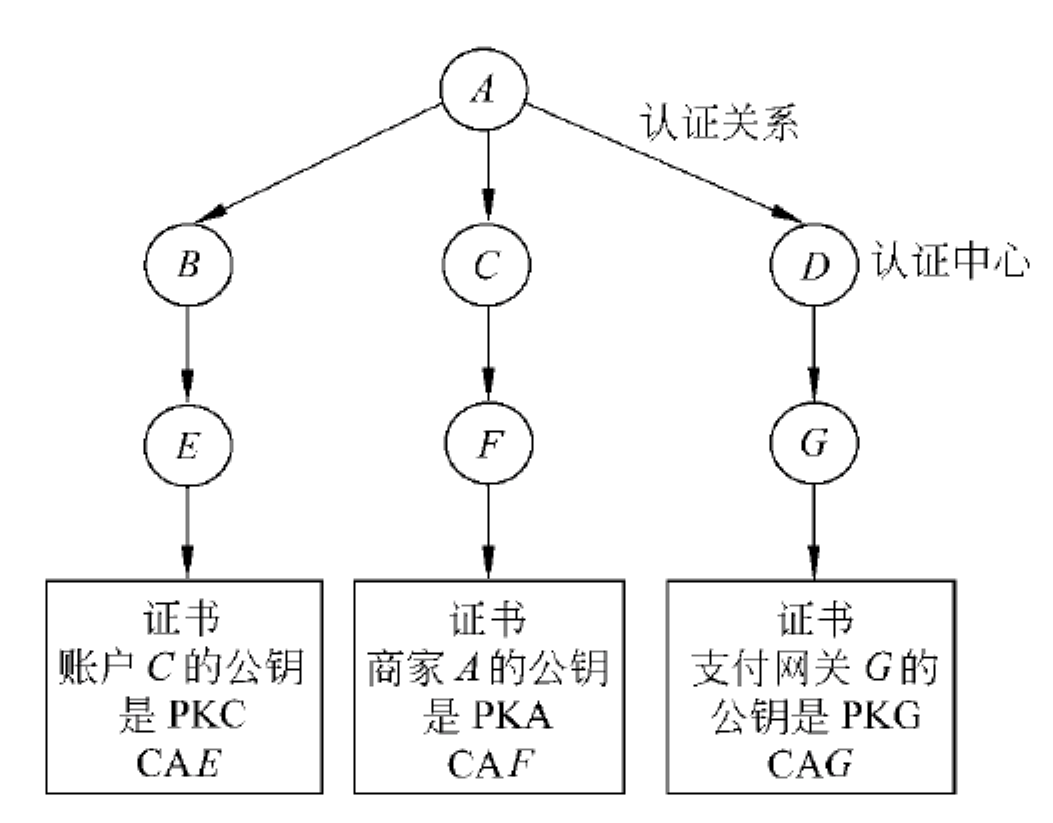
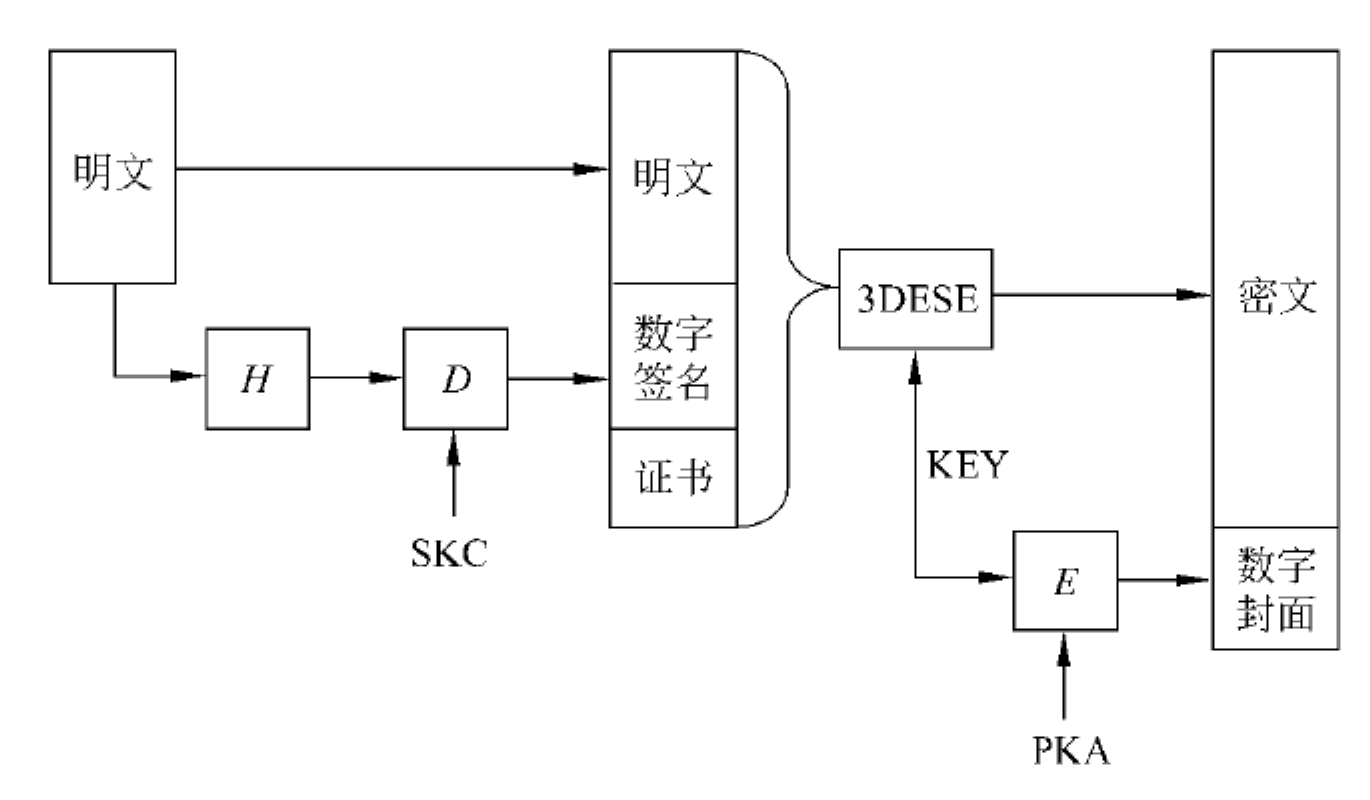


图 11.6　认证中心链

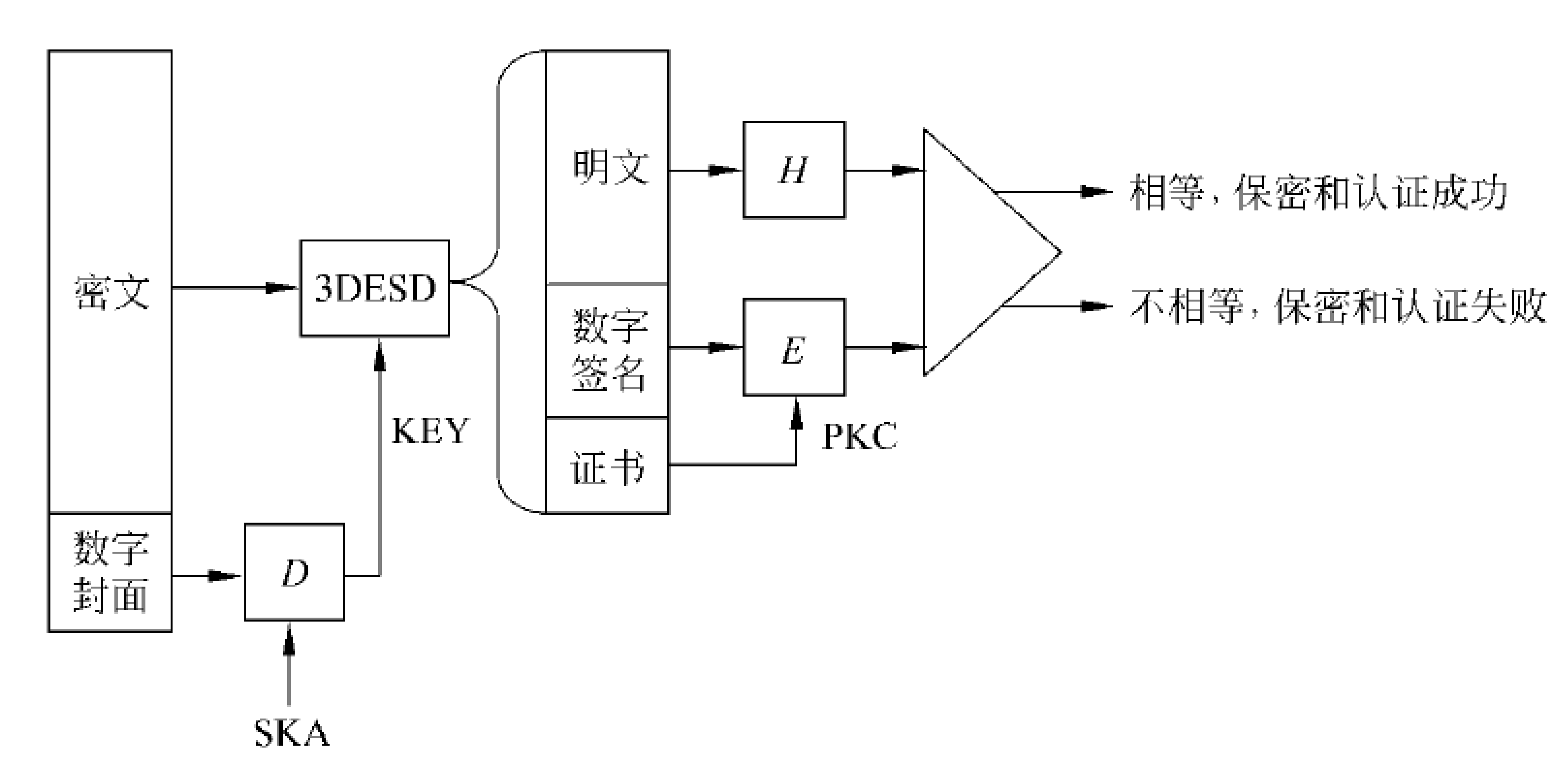
加密和认证机制的功能一是认证 SET 消息发送者的身份，二是保证只有发送者指定的接收者才能读取 SET 消息中的内容。图 11.7(a)给出持卡人发送 SET 消息给商家的过程，持卡人证书将某个信用卡关联的账户和某个公钥绑定在一起，拥有和该公钥对应的私钥的人，被确认为该信用卡的合法持有人。商家证书将商家标识符和某个公钥绑定在一起，拥有和该公钥对应的私钥的商家，被确认为商家标识符指定的商家。

发送端首先用某种报文摘要算法对 SET 消息明文进行运算，得到 SET 消息的报文摘要，然后，用持卡人的私钥 SKC 对报文摘要进行解密运算，得到持卡人的数字签名，SKC 是持卡人证书中公钥 PKC 对应的私钥。

持卡人数字签名$=D_{SKC}(H($明文$))$；H 指报文摘要算法，如 MD5 和 SHA-1，D 是



(a) 持卡人封装处理过程



(b) 商家认证持卡人身份和确认数据保密性和完整性过程

图 11.7 认证双方身份及数据保密性和完整性过程

RSA 解密算法。

持卡人将 SET 消息明文、持卡人数字签名和持卡人证书串接在一起，然后随机生成 168 位的对称密钥 KEY，用 3DES 加密算法（3DESE）和对称密钥 KEY 对串接后的结果进行加密运算。

$$密文=3DESE_{KEY}(明文 \| 持卡人数字签名 \| 持卡人证书)；\| 是串接操作符$$

对称密钥用指定接收者证书中的公钥进行加密运算，结果作为数字封面和密文一起发送给接收者。

$$数字封面=E_{PKA}(KEY)；E 是 RSA 加密算法$$

商家 A 为了读取 SET 消息，首先需要得到对称密钥 KEY，由于数字封面是用商家 A 证书中的公钥 PKA 对对称密钥 KEY 进行加密运算后得到的结果，因此，用公钥 PKA 对应的私钥 SKA 对数字封面进行解密运算就能得到对称密钥 KEY，但拥有私钥 SKA 也证明了接收者是商家 A，这就保证了只有拥有私钥 SKA 的商家 A 才能得到对称密钥 KEY。

$$KEY=D_{SKA}(E_{PKA}(KEY))；SKA 是公钥 PKA 对应的私钥$$

得到对称密钥 KEY 后，用 3DES 解密算法（3DESD）和对称密钥 KEY 还原出 SET

消息明文、持卡人数字签名和持卡人证书，用持卡人证书中的公钥 PKC 对持卡人数字签名进行加密运算，得到明文的报文摘要。

$$\text{明文报文摘要} = E_{PKC}(D_{SKC}(\text{明文报文摘要}))\text{；SKC 是公钥 PKC 对应的私钥}$$

如果接收者用同样的报文摘要算法对明文进行运算，其结果应该和用持卡人证书中的公钥 PKC 对持卡人数字签名进行加密运算后得到的结果相同。如果相同，也证明了持卡人数字签名是对明文报文摘要用持卡人证书中公钥对应的私钥进行解密运算后的结果，发送者拥有持卡人证书中公钥对应的私钥，证明了发送者就是持卡人，同时，也证明数据传输过程中没有被损坏或篡改。

4. 双重签名

持卡人完成一次电子交易需要向商家列出购买的商品清单和支付凭证，支付凭证中给出持卡人拥有的信用卡信息及付款对象和金额，由于信用卡信息对商家是保密的，因此，商家只能验证该支付凭证，不能读取支付凭证中有关信用卡账户的信息，同时，为了日后避免纠纷，无论商家，还是持卡人都需要将每一次电子交易涉及的购物清单和支付凭证绑定在一起。持卡人每一次电子交易中给出的购物清单称为订货信息（Order Information，OI），支付凭证称为支付信息（Payment Information，PI），这两种信息通过交易标识符关联在一起，即这两种信息中必须包含相同的交易标识符。持卡人必须能够向商家和支付网关证明这一次电子交易中涉及的两组信息确实由持卡人给出，为此，持卡人的数字签名不仅需要证明这一次电子交易中涉及的两组信息确实由持卡人给出，还须将这两组信息绑定在一起，实现这一功能的数字签名称为双重签名（Dual Signature，DS），整个过程如图 11.8 所示。

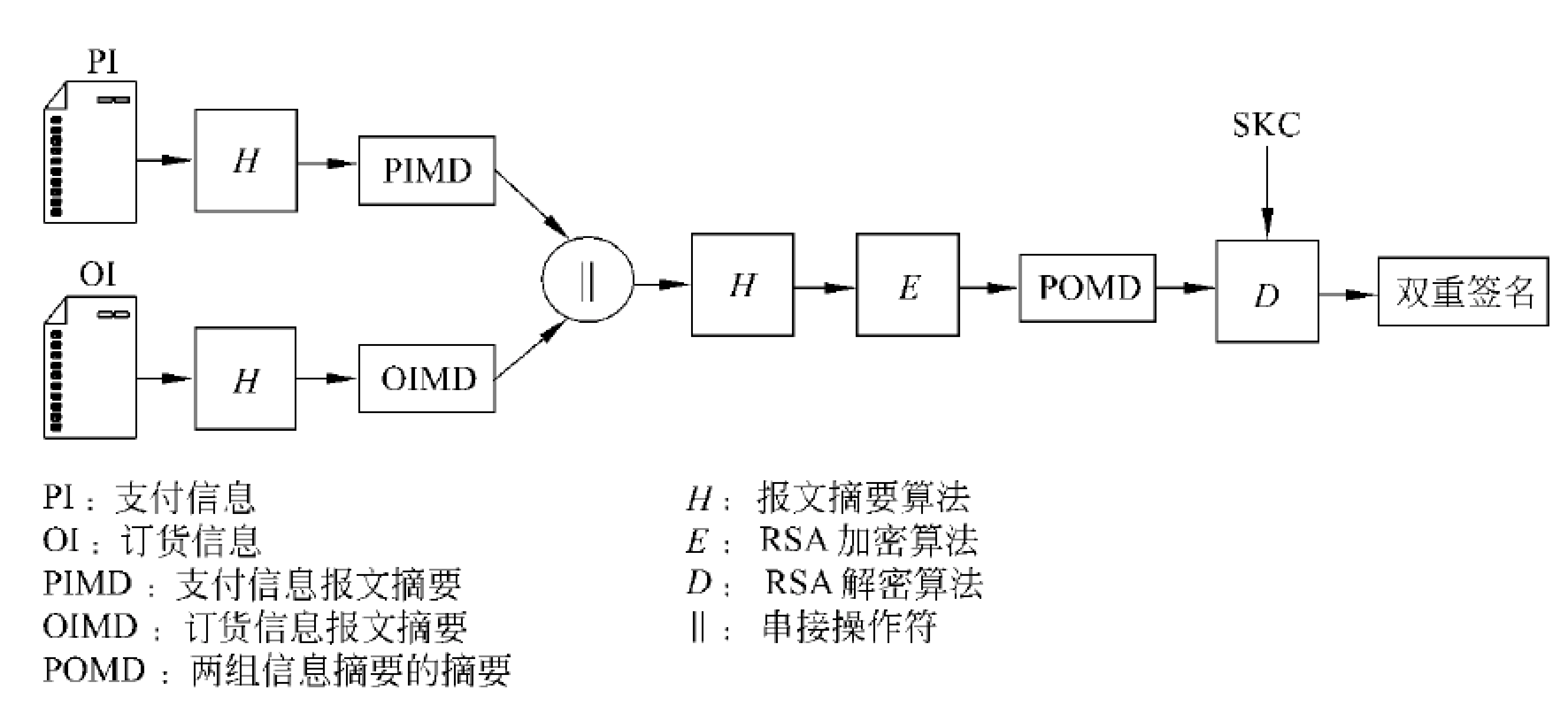


图 11.8　双重签名过程

$$\text{双重签名(DS)} = D_{SKC}(H(H(\text{PI}) \| H(\text{OI})))$$

商家是不允许获得 PI 的，这种情况下，为了验证双重签名，需要向商家提供支付信息报文摘要（PIMD），在 $H(\text{PIMD} \| H(\text{OI})) = E_{PKC}(\text{DS})$ 的情况下，确认双重签名。同样，支付网关并不需要 OI，为了验证双重签名，需要向支付网关提供订货信息报文摘要（OIMD），在 $H(\text{OIMD} \| H(\text{PI})) = E_{PKC}(\text{DS})$ 的情况下，确认双重签名。

5. 电子交易过程

1）签发证书

持卡人、商家和支付网关在开始电子交易前，必须获得认证中心签发的证书，认证中心为了签发证书，如证明持卡人信用卡账户和公钥 PKC 之间绑定关系的证书，可能需要和相关金融机构协商，但认证中心和金融机构协商过程中交换的消息属于支付系统专用消息，不是 SET 消息。

2）选择商品

持卡人通常用浏览器访问商家 Web 主页，并选择需要购买的商品，商家将持卡人的订货信息（OI）返回给持卡人，这一步并没有涉及 SET 协议。

3）初始请求和响应

持卡人接收到商家返回的订货信息后，开始电子交易过程。首先向商家发送初始请求消息（图 11.9 中消息①），消息中包含持卡人拥有的信用卡类型、发行机构，为了匹配持卡人发送的初始请求和商家返回的初始响应，还包含请求标识符和随机数，商家返回的初始响应中需要包含相同的请求标识符和随机数。请求消息作为明文经过如图 11.7(a)所示的封装处理后发送给商家。

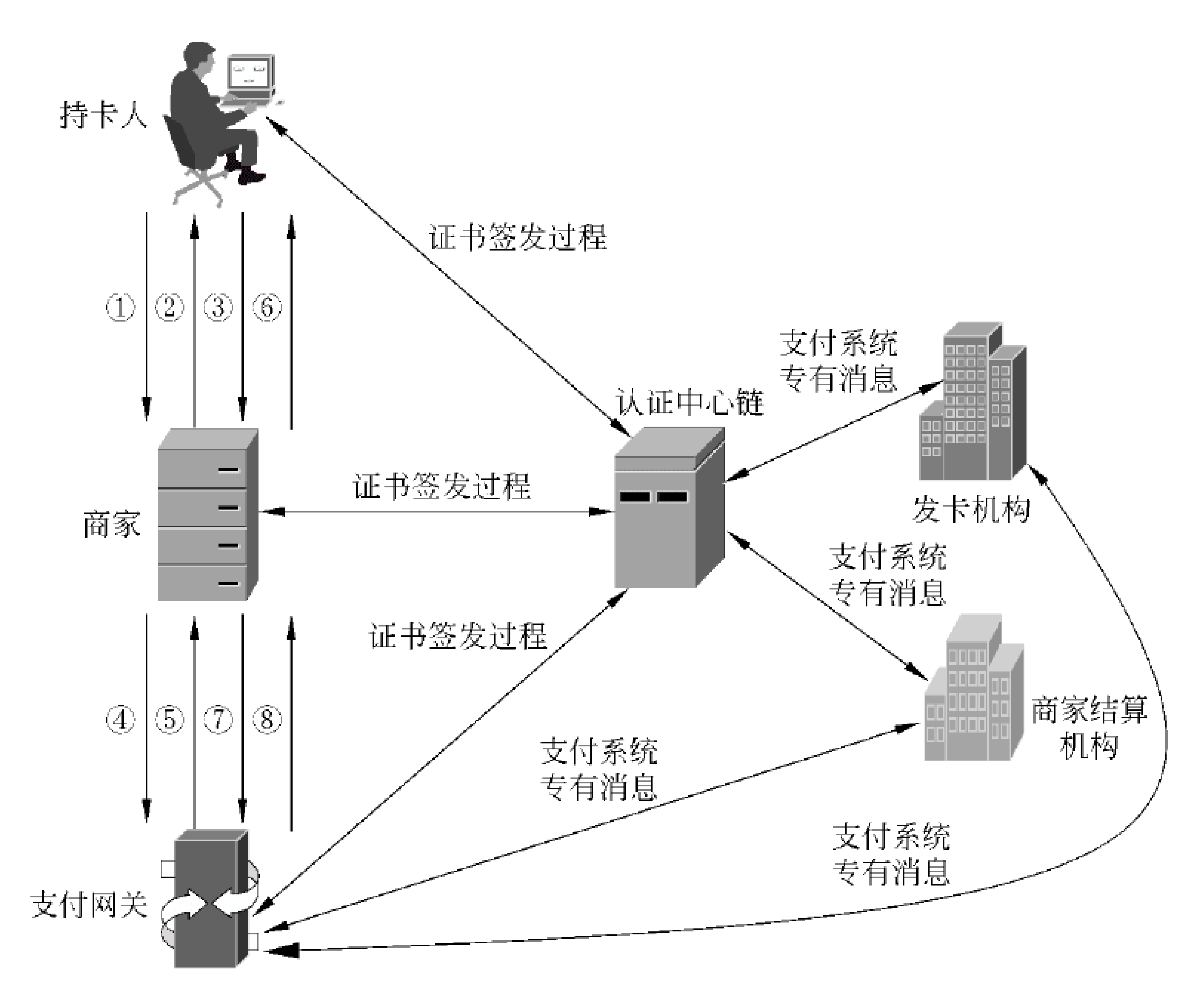


图 11.9 电子交易过程

商家接收到初始请求消息后，对初始请求消息进行如图 11.7(b)所示的持卡人签名认证和数据完整性检测，在确认无误后，向持卡人发送初始响应消息（图 11.9 中消息②），消息中包含商家为这次交易分配的交易标识符、商家和支付网关证书及用于匹配初始请求和初始响应消息的请求标识符和随机数。在 SET 消息交换过程中，发送者对发送消息进行如图 11.7(a)所示的封装处理，当然，数字签名用的私钥是发送者拥有的私钥，加密对称密钥

KEY 的公钥是接收者的公钥，每一次随机生成的对称密钥 KEY 是不同的。同样，接收者对接收到的 SET 消息进行图 11.7(b)所示的发送者签名认证和数据完整性检测。

4）购买请求

持卡人获得购物清单、本次交易金额、本次交易标识符、商家和支付网关证书后，构建支付信息(PI)和订货信息(OI)，并将它们封装成购买请求消息(图 11.9 中消息③)，发送给商家，整个封装处理过程如图 11.10 所示。支付信息用于让支付网关实现持卡人账户至商家账户的电子转账，由于包含信用卡账户信息，只允许支付网关读取支付信息。订货信息用于向商家确认购货清单。为了将订货信息和支付信息绑定在一起，它们均包含本次交易标识符，而且持卡人采用双重签名方式：

双重签名$=D_{SKC}(H(H(PI) \| H(OI)))$

其中，SKC 是持卡人的私钥；H 是报文摘要算法，如 MD5 或 SHA-1；D 是 RSA 的解密算法。

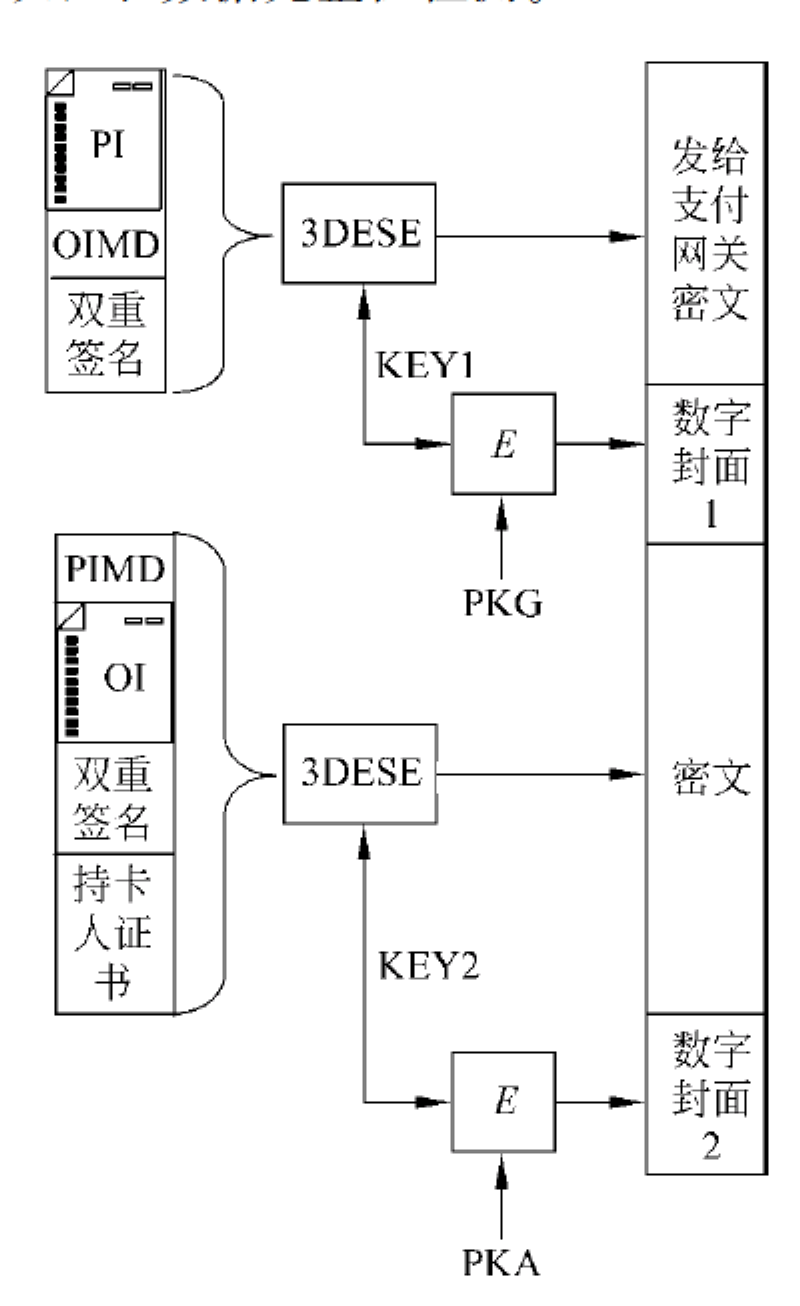


图 11.10　购买请求消息封装处理过程

为了加密经由商家转发给支付网关的信息，持卡人随机生成 168 位对称密钥 KEY1，并用 3DES 加密算法(3DESE)对这些信息进行加密，得到发送给支付网关的密文。

发送给支付网关的密文$=3DESE_{KEY1}(PI \|$双重签名$\| OIMD)$；$OIMD=H(OI)$

为了保证支付网关能够还原出持卡人发送给它的信息，用支付网关的公钥 PKG 加密 KEYI 后，生成数字封面 1，并将数字封面 1 添加在发送给支付网关的密文后。

数字封面 1$=E_{PKG}(KEY1)$；E 是 RSA 的加密算法

同样，持卡人发送给商家的订货信息和 PIMD(PIMD$=H(PI)$)也采用双重签名方式，如果只允许商家获悉订货信息，还需用 3DES 加密算法(3DESE)和对称密钥 KEY2 对持卡人发送给商家的信息进行加密，并用商家的公钥 PKA 加密 KEY2 后，生成数字封面 2，并将数字封面 2 一起发送给商家。

商家接收到持卡人发送的购买请求消息后，进行如图 11.11 所示的认证和数据完整性检测过程。首先解密出订货信息、双重签名和持卡人证书等，然后通过比较 $H(H(OI) \| PIMD)$ 和 E_{PKC}(双重签名)是否相等来认证双重签名，如果相等，表明 OI 和 PIMD 确实由持卡人发送，且这些信息传输过程中没有损坏，同时，证明双重签名有效。

证明双重签名有效后，商家处理订货信息，在决定向持卡人提供订货信息要求的货物或服务前，需要通过支付网关确认持卡人账户的有效性，是否有能力支付该次交易所需金额。因此，向支付网关发送用于确认持卡人支付能力的授权请求消息。

6. 授权请求和响应

商家发送给支付网关的授权请求消息(图 11.9 中消息④)主要包含两部分内容：一是持卡人需要商家转发的发送给支付网关的密文，它是对持卡人发送给支付网关的支付

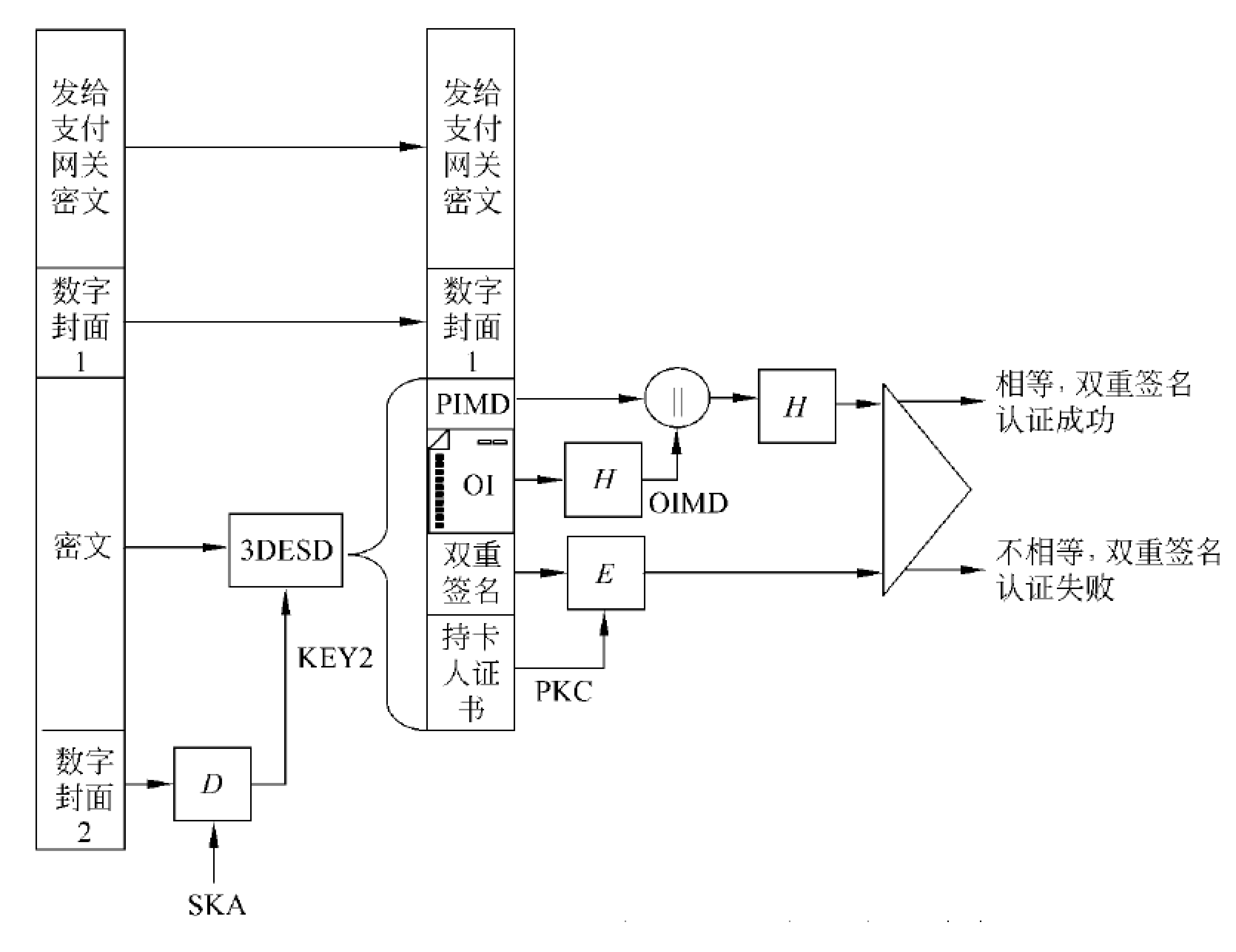


图 11.11 商家认证购买请求消息过程

信息、双重签名和 OIMD 进行加密运算后的结果。二是商家需要支付网关确认的授权信息，其中包含本次交易标识符、持卡人本次交易需要支付的金额等，这些信息由商家数字签名后，还需用 3DES 加密算法(3DESE)和对称密钥 KEY3 对这些信息进行加密，并用支付网关的公钥 PKG 加密 KEY3 生成数字封面 3，并将数字封面 3 一起发送给支付网关，整个封装处理过程如图 11.12 所示。

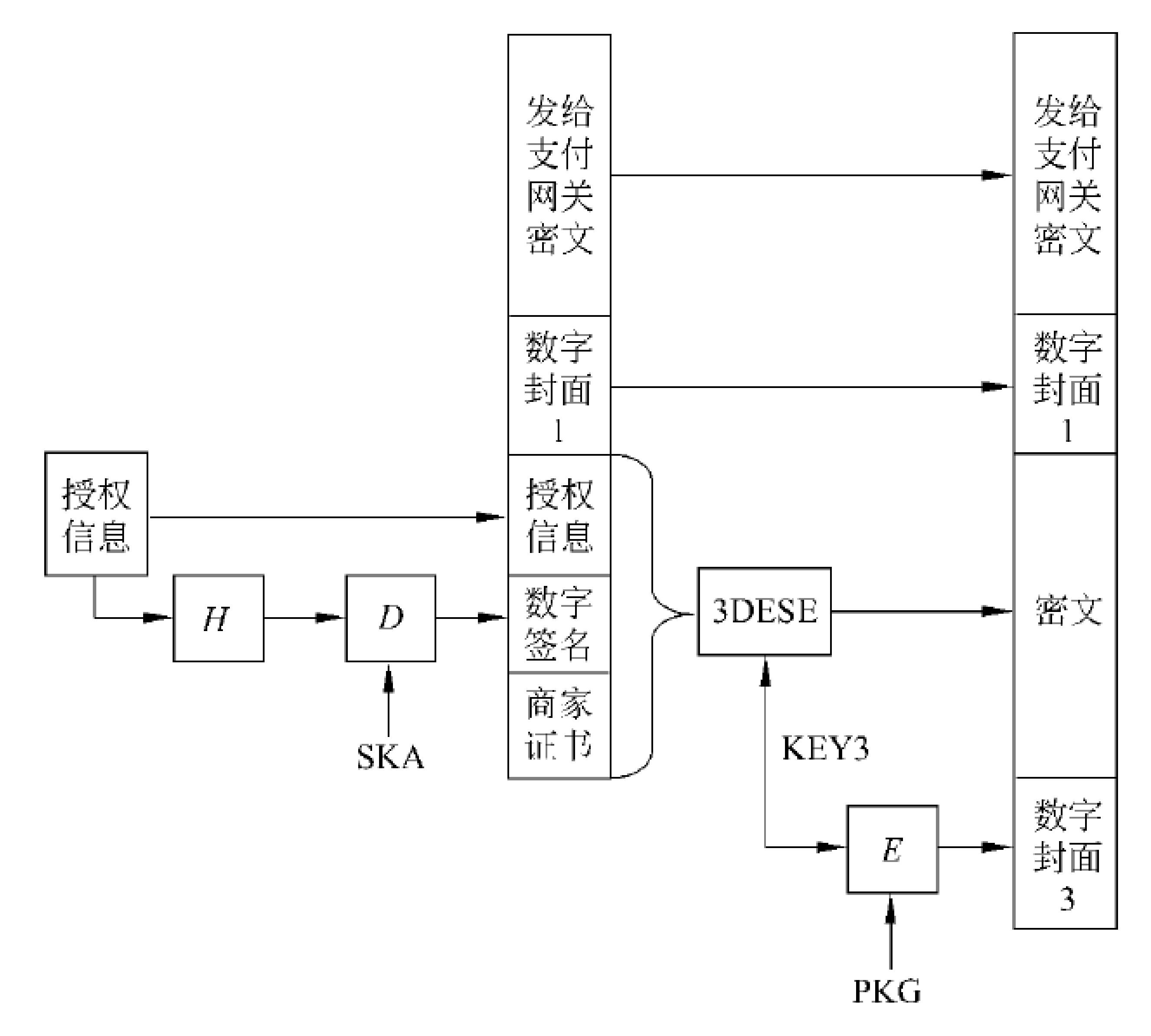


图 11.12 授权请求消息封装处理过程

$$密文=3DESE_{KEY3}(授权信息 \| 数字签名 \| 商家证书)$$

$$数字签名=D_{SKA}(H(授权信息))$$

$$数字封面\ 3=E_{PKG}(KEY3)$$

支付网关接收到授权请求消息后，进行如图 11.13 所示的认证和数据完整性检测过程，首先认证持卡人的双重签名，比较 $H(H(PI) \| OIMD)$ 和 E_{PKC}(双重签名)，如果相等，表示 PI 和 OIMD 确实由持卡人发送，且这些信息传输过程中没有损坏，同时，证明双重签名有效。为了证明授权信息确实由商家发送，验证解密后的授权信息和数字签名，比较 H(授权信息)和 E_{PKA}(数字签名)，如果相等，表示授权信息确实由商家发送，且这些信息传输过程中没有损坏，同时，证明商家的数字签名有效。

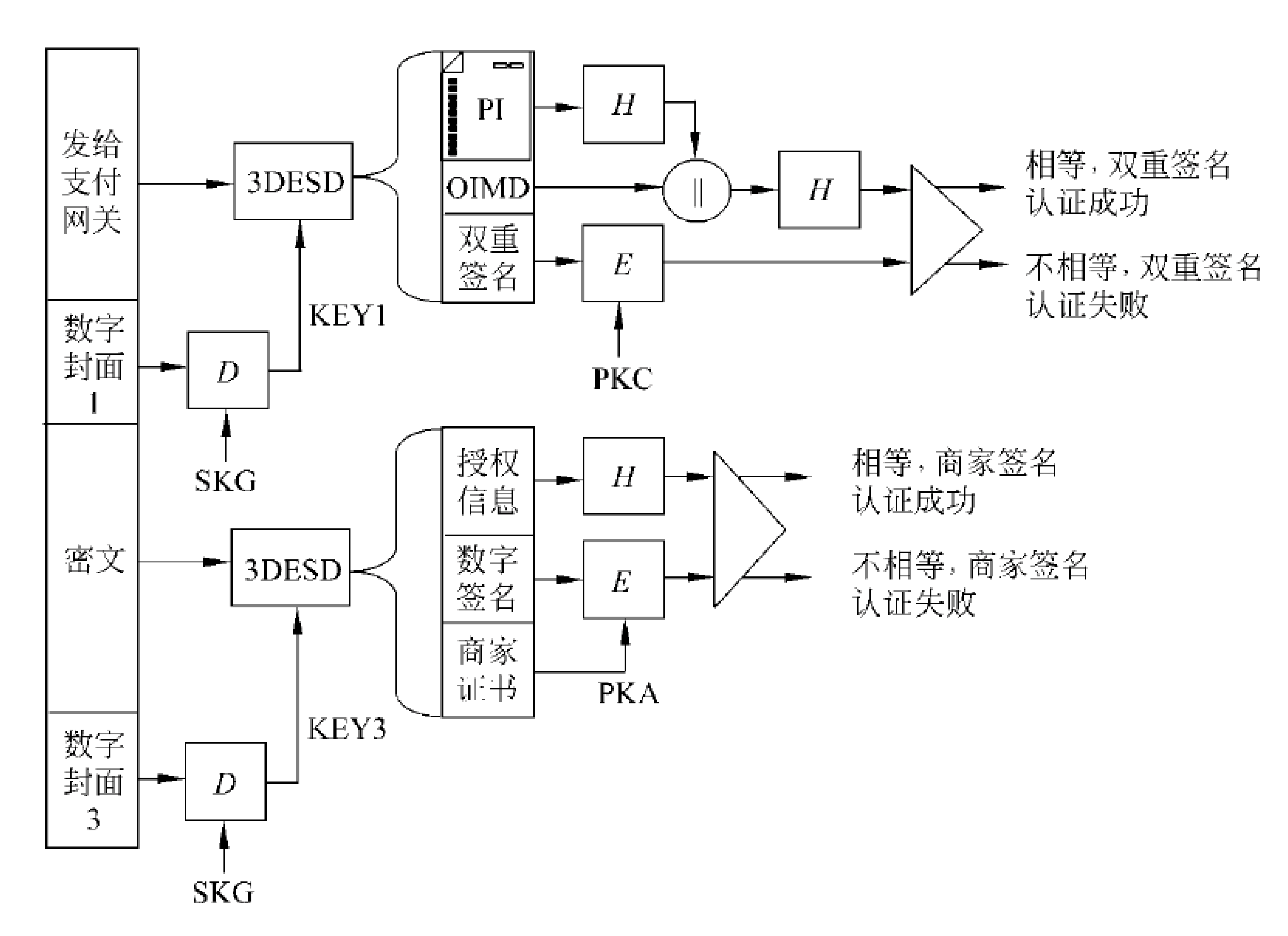


图 11.13　支付网关认证授权请求消息过程

完成认证后，支付网关比较授权信息和 PI，确定两组信息中交易标识符和支付金额相同的情况下，通过支付网络和金融机构的支付系统向发卡机构求证持卡人账户的支付能力，证实持卡人账户具有该次交易所需金额的支付能力后，向商家发送授权响应消息(见图 11.9 中消息⑤)。

授权响应消息封装处理过程如图 11.14 所示，它包含两部分信息，一是授权信息，用于告知商家要求支付网关求证的持卡人支付能力已经得到证实。二是支付网关的承兑凭证，表示支付网关随时可以实现授权信息给出的本次交易所需金额的电子转账。授权信息和承兑凭证都由支付网关签名，但由于加密承兑凭证的对称密钥 KEY4 由支付网关的公钥 PKG 加密，因此，只有支付网关才能验证承兑凭证。承兑凭证成为商家向持卡人提供本次交易所需货物或服务后，要求支付网关完成本次交易所需金额的电子转账的凭证，不允许商家对其进行处理。

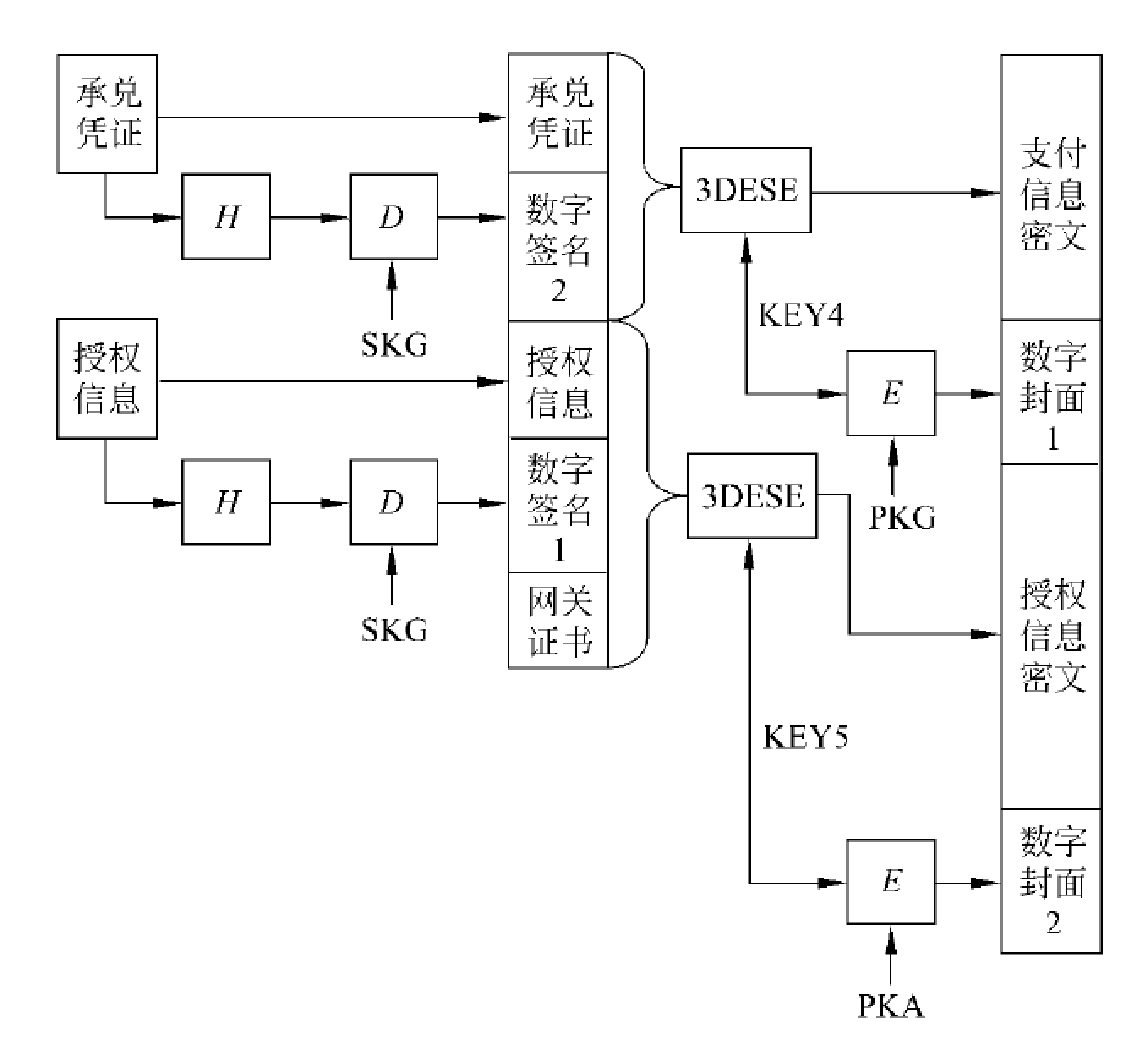


图 11.14 授权响应消息封装处理过程

数字签名 1=D_{SKG}(H(承兑凭证))

数字签名 2=D_{SKG}(H(授权信息))

支付信息密文=$3DESE_{KEY4}$(承兑凭证‖数字签名 1)

数字封面 1=E_{PKG}(KEY4)

授权信息密文=$3DESE_{KEY5}$(授权信息‖数字签名 2‖网关证书)

数字封面 2=E_{PKA}(KEY5)

显然,商家只能认证授权信息的数字签名,证实授权信息由支付网关发送,保留支付信息密文,用于要求支付网关实现本次交易所需金额的电子转账时使用。商家向持卡人发送购货响应消息(见图 11.9 中消息⑥),同时,开始向持卡人提供本次交易要求的货物或服务。

7. 购货响应

购货响应消息包含商家确认持卡人订货信息的内容,这些确认信息由商家进行如图 11.7(a)所示的数字签名和加密处理后,发送给持卡人,持卡人对其进行如图 11.7(b)所示的签名认证和完整性检测,确认本次交易涉及的网络操作部分成功完成。

8. 支付请求和响应

商家向持卡人提供本次交易要求的货物或服务后,通过向支付网关发送支付请求消息(见图 11.9 中消息⑦)请求支付网关实现本次交易所需金额的电子转账,支付请求消息包含两部分信息,一是支付网关包含在授权响应消息中的承兑凭证;二是支付请求信息,其中给出本次交易标识符、支付金额等,支付请求消息经过如图 11.15 所示的签名和加密处理后,发送给支付网关。

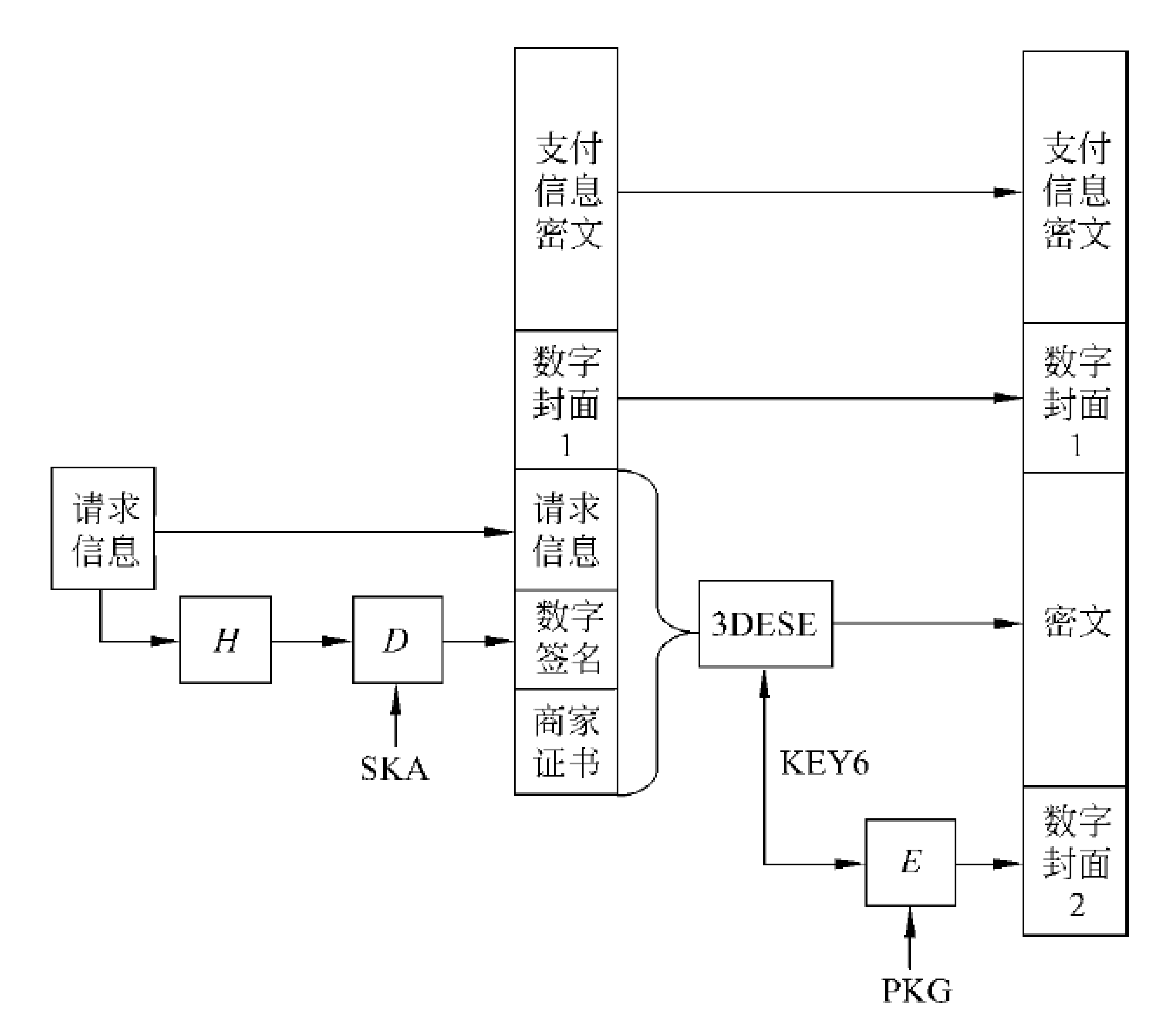


图 11.15　支付请求消息封装处理过程

数字签名$=D_{SKA}(H($支付请求信息$))$

密文$=3DESE_{KEY6}($支付请求信息 ‖ 数字签名 ‖ 商家证书$)$

数字封面 2$=E_{PKG}(KEY6)$

支付网关接收到支付请求消息后，完成对支付请求信息的数字签名认证和完整性检测，同时，完成对承兑凭证的签名认证和完整性检测，在确认承兑凭证没有损坏，支付请求信息中的交易标识符和支付金额与承兑凭证给出的相同，通过支付网络和支付系统要求金融机构完成电子转账，在确认金融机构完成电子转账的情况下，向商家发送支付响应消息（见图 11.9 中消息⑧）。商家接收到支付响应消息后，完成本次交易过程，保留支付响应消息，作为日后和支付网关对账的凭证。同样，支付响应消息在发送时需要经过图 11.7(a)所示的签名和加密处理过程，商家接收到支付响应消息后，也需要进行图 11.7(b)所示的签名认证和完整性检测。

11.2　电子邮件安全协议

11.2.1　PGP

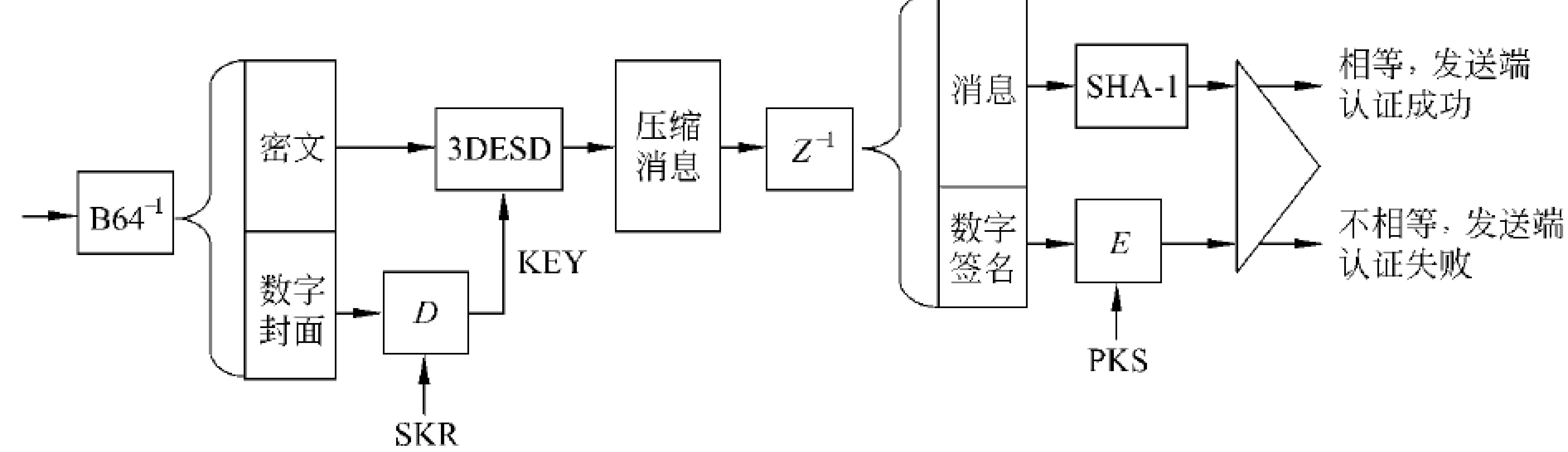
PGP(Pretty Good Privacy)是一种安全传输电子邮件的技术，它主要实现发送端认证、消息压缩、加密及码制转换等功能。发送端数字签名、压缩、加密及 Base64 编码过程如图 11.16(a)所示，接收端 Base64 解码、解密、解压和发送端认证过程如图 11.16(b)所示。当然，用户可以只选择其中一项或多项功能，如只认证，不压缩和加密。

1. 数字签名和认证

数字签名和认证用于确认消息的发送者，发送者发送消息前计算数字签名：

消息
SHA-1
D
SKS
消息
数字签名
Z
压缩消息
3DESE
KEY
E
PKR
密文
数字封面
B64

(a) 发送端处理过程



(b) 接收端处理过程

图 11.16 PGP 操作过程

$$数字签名 = D_{SKS}(SHA\text{-}1(消息))$$

其中，SKC 是发送端 RSA 不对称密钥对中的私钥，D 是 RSA 的解密算法。

发送端将数字签名附在消息后面一起发送给接收端，接收端为了认证数字签名，必须拥有发送端 RSA 不对称密钥对中的公钥(这里为 PKS)，然后比较 SHA-1(消息)和 E_{PKS}(数字签名)，如果两者相等，接收端确认消息的发送者，并确认数据传输过程中没有损坏。如果发送端存在多对 RSA 不对称密钥对，则需要给出用于确定认证用公钥的信息。比较直接的办法是给出证明公钥和发送者之间绑定关系的证书，如 SET，但证书的信息量较大，影响传输效率。PGA 在数字签名字段中附加公钥标识符，它实际上是认证数字签名的公钥的低 64 位，这样，发送者必须为自己使用的多对 RSA 不对称密钥对建立 RSA 不对称密钥对索引表，索引表中包含以下字段：

- 生成时间：RSA 不对称密钥对生成时间。
- 公钥：RSA 不对称密钥对中的公钥。
- 私钥：RSA 不对称密钥对中的私钥。
- 公钥标识符：公钥的低 64 位。
- 用户标识符：发送者标识符，通常是发送者的 E-mail 地址。

同样，接收者需要对应每一个发送者建立公钥索引表，索引表中包含如下字段：

- 时间戳：该索引项生成时间。
- 公钥标识符：用于检索对应的公钥。
- 公钥;认证数字签名用的公钥。
- 用户标识符：发送者标识符，通常是发送者的 E-mail 地址。

发送者计算数字签名前，先在 RSA 不对称密钥对索引表中选择一对 RSA 不对称密钥对，用私钥进行数字签名，并在数字签名后附加公钥标识符。接收端认证数字签名前，用公钥标识符检索公钥索引表，找到对应的公钥，然后进行数字签名认证。

2. 压缩和解压

消息和数字签名在加密前，用压缩算法进行压缩，得到压缩消息。

$$\text{压缩消息} = Z(\text{消息} \parallel \text{数字签名})$$

解压操作是压缩操作的逆操作，用 Z^{-1} 表示。

$$\text{消息} \parallel \text{数字签名} = Z^{-1}(\text{压缩消息})$$

3. 加密和解密

PGP 支持多种加密算法，图 11.16 假定采用 3DES 作为加密算法，发送端随机生成 168 位对称密钥 KEY，然后用对称密钥 KEY 和 3DES 加密算法（3DESE）加密压缩消息，得到密文。

$$\text{密文} = 3\text{DESE}_{\text{KEY}}(\text{压缩消息})$$

对称密钥 KEY 是一次性密钥，只用于加密这一次传输的数据，由于 3DES 是对称密钥加密算法，必须用同一个密钥进行解密处理，因此，发送端必须将用于加密的对称密钥 KEY 传输给接收端，当然，密钥不能以明文方式传输，而且只允许接收端能够还原出对称密钥 KEY，因此，用接收端拥有的某对 RSA 不对称密钥对中的公钥加密对称密钥 KEY 后，生成数字封面。

$$\text{数字封面} = E_{\text{PKR}}(\text{KEY})$$

其中，E 是 RSA 加密算法，PKR 是接收端拥有的某对 RSA 不对称密钥对中的公钥。

接收端为了解密密文，首先需要还原出对称密钥 KEY，然后用对称密钥 KEY 解密密文。

$$\text{KEY} = D_{\text{SKR}}(\text{数字封面})$$

其中，D 是 RSA 解密算法，SKR 是公钥 PKR 对应的私钥。

如果接收端存在多对 RSA 不对称密钥对，发送端需要在数字封面字段中附加公钥标识符，它是发送端加密对称密钥 KEY 时选择的公钥的低 64 位，接收端首先需要用公钥标识符检索 RSA 不对称密钥对索引表，找到对应的私钥，然后用私钥还原出对称密钥 KEY。

接收端还原出对称密钥后，用 3DES 解密算法（3DESD）解密密文，得到压缩消息。

$$\text{压缩消息} = 3\text{DESD}_{\text{KEY}}(\text{密文})$$

4. Base64 编码和解码

经过数字签名、压缩、加密处理后形成的是任意二进制位流，而许多电子邮件系统只允许传输可打印的 ASCII 字符，因此，发送端需要经过 Base64 编码将任意二进制位流转换成可打印的 ASCII 字符流。同样，接收端在进行解密、解压和数字签名认证前，需要进行 Base64 解码，把可打印的 ASCII 字符流还原成 Base64 编码前的二进制位流。

11.2.2　S/MIME

S/MIME（Secure/Multipurpose Internet Mail Extension）是在通用 Internet 邮件扩

充(Multipurpose Internet Mail Extension,MIME)邮件格式的基础上增加了和安全传输邮件相关的内容类型后的邮件格式,增加的内容类型主要为了表示用于认证邮件内容的数字签名和加密邮件内容产生的密文。采用的认证算法、加密算法和报文摘要算法与PGP使用的大致一致,如用RSA或DSS作为数字签名算法,用三重DES(3DES)作为加密算法,用SHA-1或MD5作为报文摘要算法。在讨论S/MIME邮件格式前,先简单回顾一下SMTP和MIME邮件格式。

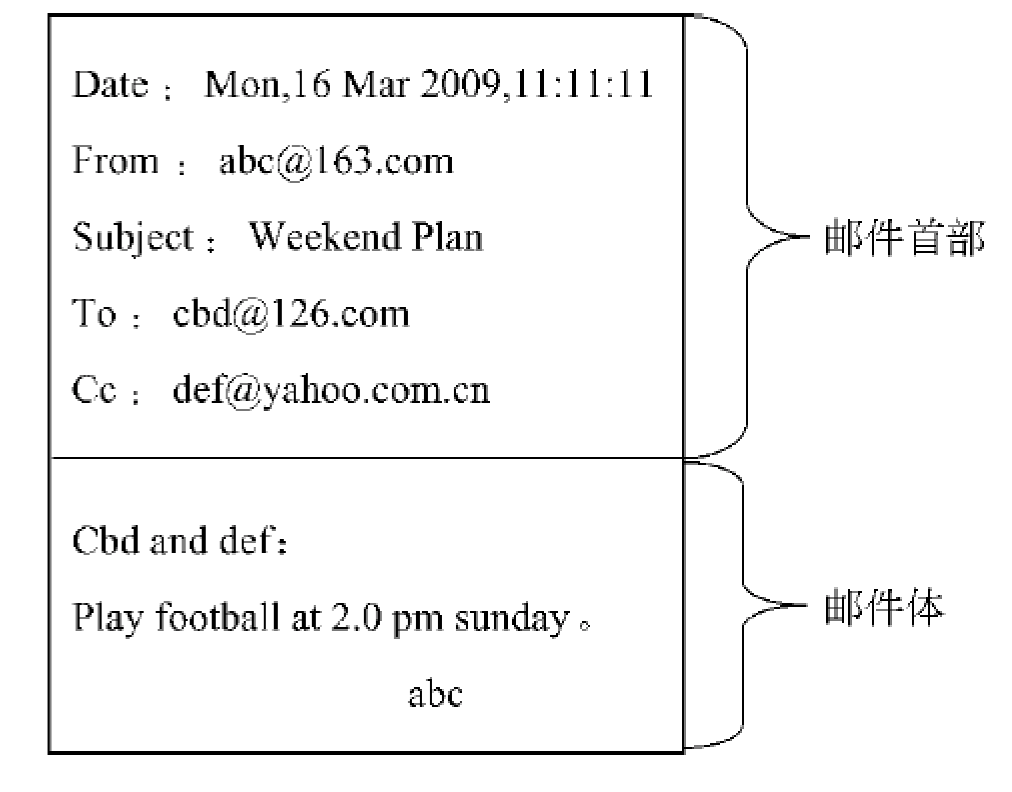


图 11.17 SMTP 邮件格式

1. SMTP 邮件格式

SMTP邮件首部由关键词和参数组成,中间用冒号分隔。常见的关键词如下:

- Date 给出邮件发送日期、时间。
- From 给出发件人名称和邮箱地址。
- Subject 给出邮件主题,用于向收件人提示邮件内容。
- To 给出收件人邮箱地址。
- Cc 一封邮件可以抄送给多个收件人,给出抄送者的邮箱地址。

SMTP邮件体给出邮件内容。SMTP只能传输7位ASCII码,因此,无法传输由任意二进制位流构成的邮件体,如可执行文件和包含非英语国家文字的文档。为了解决这一问题,提出了通用Internet邮件扩充(Multipurpose Internet Mail Extension,MIME)。

2. MIME 邮件格式

MIME主要包括以下三部分内容:

- 五个新的邮件首部字段,用于提供有关邮件体的信息;
- 定义了多种邮件内容格式,对多媒体电子邮件的表示方法进行了标准化;
- 定义了传送编码,可对任何内容格式进行转换,使其能够被SMTP邮件系统正常传输。

图11.18给出了MIME和SMTP的关系,发送用户需要传输的邮件内容可以是任何二进制位流,这些内容被组织成MIME格式,然后转换成适合经过SMTP邮件系统传输的编码格式。同样,接收端SMTP代理首先将邮件内容还原成MIME格式,然后提交给接收用户,接收用户从MIME格式中提取出由任意二进制位流组成的邮件内容。

MIME邮件格式如图11.19所示,它在SMTP首部的基础上增加了五个首部,分别是:

- MIME-Version 版本号,目前为1.0。
- Content-Type 通过类型/子类型参数说明邮件体内容类型。
- Content-ID 内容标识符,唯一标识指定邮件内容。
- Content-Transfer-Encoding 用于说明实际传送的邮件的编码方式。
- Content-Description 描述邮件体对象的可读字符串。

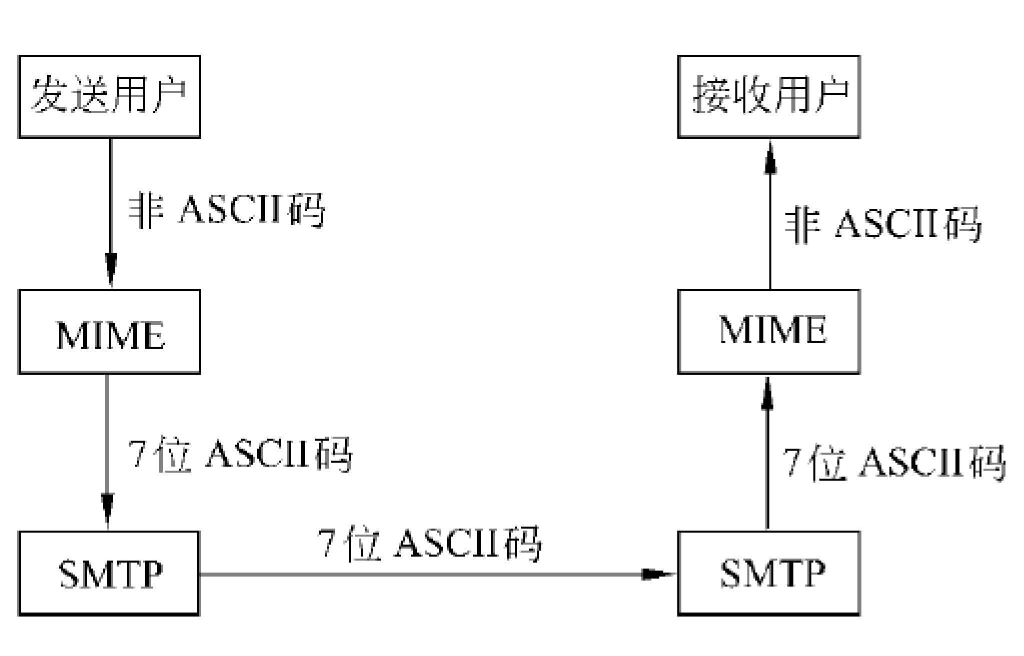




图 11.18　MIME 和 SMTP 的关系



图 11.19　MIME 邮件格式

表 11.2 给出了 MIME 支持的邮件体内容类型，可以看出，MIME 邮件体不再仅仅由标准 ASCII 码组成，可以是任意二进制位流，包括图像、动画和音频。表 11.3 给出了编码邮件体内容的编码方式，最常用的是 Base64 编码，它将任意二进制位流以 6 位为单位分组，在 ASCII 字符集中选择 64 个可打印字符，对应 6 位二进制数的 64 种不同的值。每一种 6 位二进制数值用对应的 8 位可打印 ASCII 码表示，以此将邮件体任意二进制位流编码为一组可打印的 ASCII 字符。

表 11.2　MIME Content-Type 参数组合及含义

类　　型	子　类　型	说　　明
Text	Plain	无格式文本，简单 ASCII 字符串
	Enriched	提供较多格式灵活性的文本类型
Multpart	Mixed	邮件由多个子报文组成，多个不同子报文相互独立，但一起传输，并按照在邮件中的顺序提供给收件人
	parallel	和 Mixed 基本相同，但提供给收件人时，没有给各个子报文定义顺序
	Alternative	不同子报文是同一信息的不同版本，提供最佳版本给收件人
	Digest	和 Mixed 基本相同，但每一个子报文是一个完整的 rfc822 邮件
Message	rfc822	rfc822 邮件
	Partial	为传输一个超大邮件，以对收件人透明的方式分割邮件
	External-body	包含一个指向存储在其他地方的对象的指针
Image	jpeg	JPEG 格式图像，JFIF 编码
	gif	GIF 格式图像
Video	mpeg	MPEG 格式动画
Audio	Basic	单通道 8 位 μ 律编码，8kHz 采样速率
Application	PostScript	Adobe Postscript
	Octet-stream	不间断字节流

表 11.3 MIME 传送编码

编　码	说　明
7b	数据由短行(每行不超过 1000 字符)的 7 位 ASCII 字符表示
8b	存在非标准 ASCII 字符,即最高位置 1 的 8 位字节
binary	不仅允许包含非标准 ASCII 字符,而且每行长度可以超过 1000 字符
quoted-printable	一种既实现用 ASCII 字符表示数据,又尽可能保持原来的可读性的编码
Base64	一种用 64 个 8 位二进制表示的可打印 ASCII 字符,表示任意 6 位二进制数的编码
x-token	用于命名非标准编码

```
Date: Mon,16 Mar 2009,11:11:11
From: abc@163.com
Subject: Weekend Plan
To: cbd@126.com
Cc: def@yahoo.com.cn
MIME-Version:1.0
Content-Type:multipart/mixed;boundary=ZZYYXX

--ZZYYXX
ABC 和 DEF:
周末郊外踏青,后面附郊外风景照
                              ABC

--ZZYYXX
Content-Type:image/gif
Content-Transfer-Encoding:base64
(风景照像素数据)

--ZZYYXX--
```

以上是一个 MIME 邮件,它由两个独立的子报文组成,一个只包含字符信息的子报文和一个包含图像数据的子报文,首部中关键词 Content-Type:后面的参数 multipart/mixed 说明了这一点。boundary=ZZYYXX 定义了分隔字符串,如果出现紧跟两个连字符“--”后面的字符串“ZZYYXX”,表明新的子报文开始。分隔字符串后面紧跟两个连字符“--”,表明整个 multipart 结束。

3. S/MIME 安全机制

S/MIME 增加了几种和安全传输邮件有关的内容类型,如用于认证邮件子报文内容的 Content-Type:Application/signedData 和用于加密邮件子报文内容的 Content-Type:Application/envelopedData,认证邮件子报文内容的过程如图 11.20 所示,邮件子报文和加密后的子报文摘要(数字签名)、报文摘要算法标识符(SHA-1)、数字签名算法标识符(RSA)、签名者证书构成邮件体的一部分,为了和 SMTP 邮件传输系统兼容,对其进行 Base64 编码后作为实际发送的邮件子报文内容。加密邮件子报文内容的过程如图 11.21 所示,加密邮件子报文后生成的密文和加密对称密钥后生成的数字封面、加密算

法标识符(3DES)、加密密钥算法标识符(RSA)、用于证明加密密钥用公钥的证书构成邮件体的一部分，为了和 SMTP 邮件传输系统兼容，对其进行 Base64 编码后作为实际发送的邮件子报文内容。如果需要对邮件内容同时进行数字签名和加密操作，如图 11.20 和图 11.21 所示的过程可以嵌套，即可以先进行数字签名，然后对包括数字签名的邮件内容进行加密，反之，也可以先进行加密，然后对密文进行数字签名。

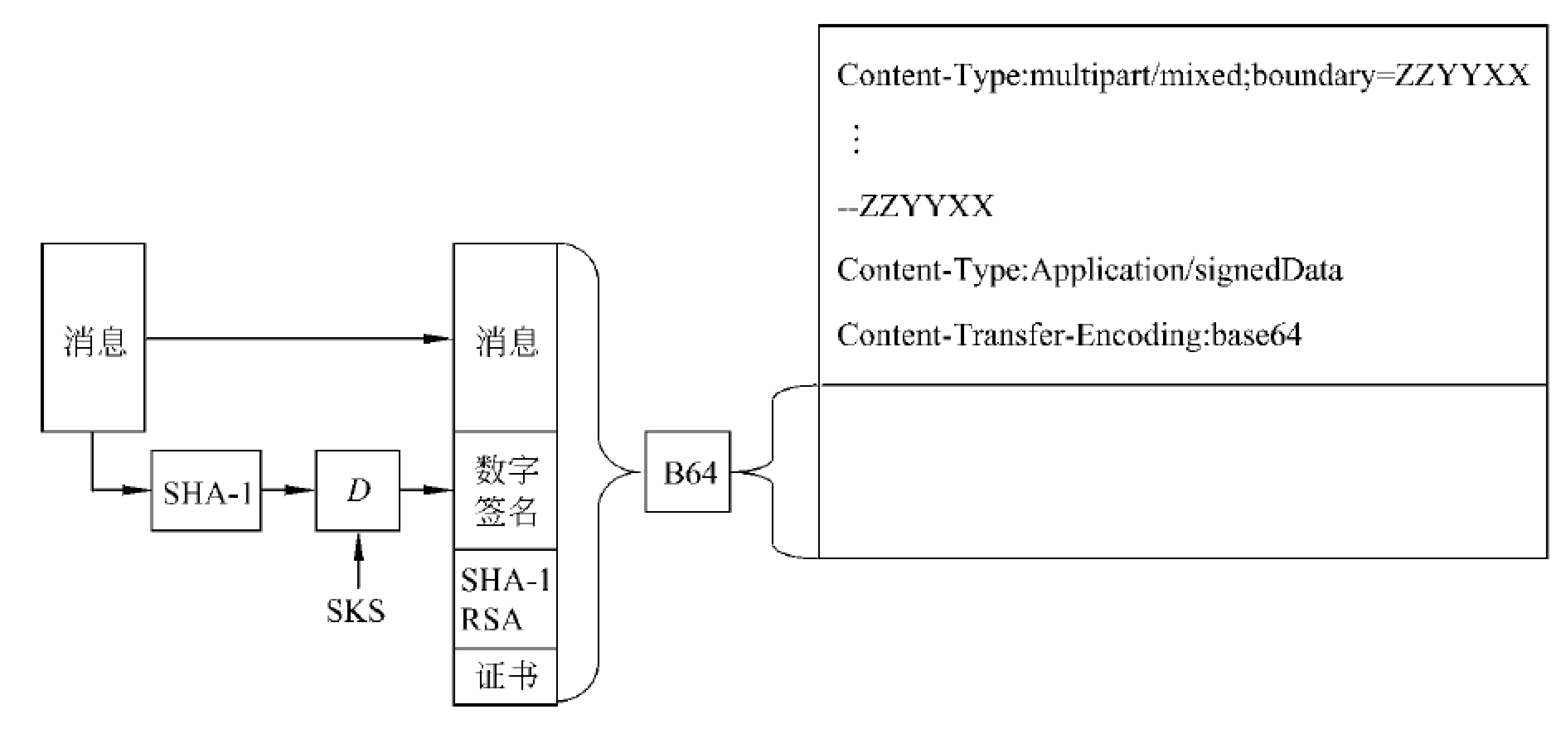


图 11.20　认证邮件子报文过程

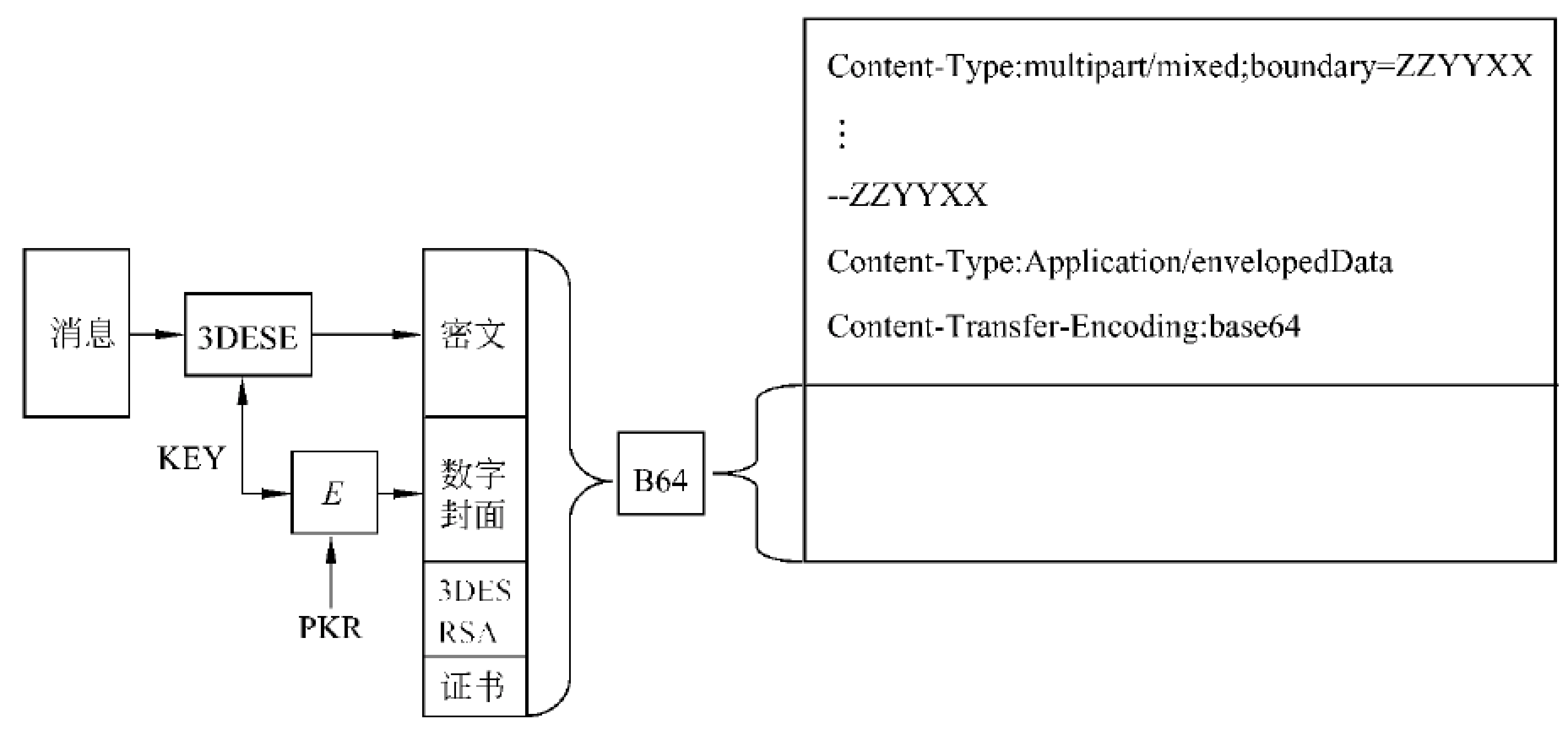


图 11.21　加密邮件子报文过程

11.3　门户网站

企业网一般分为内部网络(信任区)、非军事区和外部网络三部分，非军事区是企业为外部网络终端提供信息服务的地方，由外部网络终端发起的访问过程可以访问存放在非军事区的网络资源，通常情况下，是不允许由外部网络终端发起的访问内部网络资源的访问过程，而只能由外部网络终端向内部网络终端响应访问结果。但实际应用过程中，存在外部网络终端主动发起访问内部网络资源的访问过程的需要，如企业的合作者需要通过

Internet 获取企业内部网络资源,出差在外的企业员工,也只能通过 Internet 获取工作所需的企业内部网络资源。图 11.22 是基于 VPN 技术实现外部网络终端接入内部网络的过程,这种情况下,防火墙连接外部网络的端口就是一个虚拟的接入服务器,能够完成对外部网络终端的身份认证和 IP 地址分配,当然,分配的是内部网络的本地 IP 地址,完成接入过程的外部网络终端可以像内部网络终端一样访问内部网络资源。这种方式的最大问题是防火墙只能保证授权终端接入内部网络,但无法对授权终端访问内部网络的权限进行控制。另外,内部网络资源也是分散的,往往分布在多个 Web、FTP 和数据库服务器中,而且,不同信息资源有着不同的访问权限,这些访问权限的控制由各自的服务器应用软件实现,这样做一是重复,二是缺乏一致性。

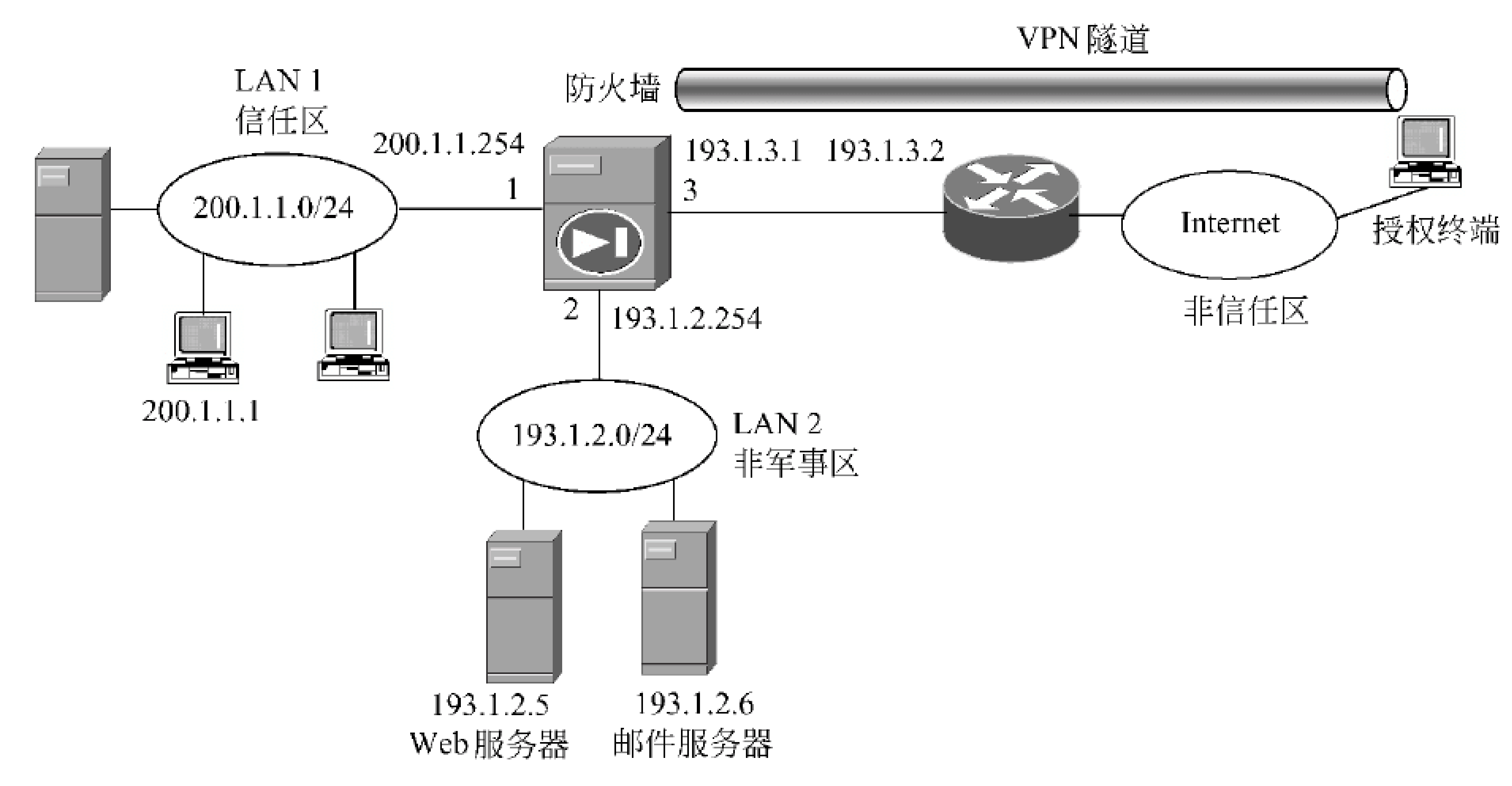


图 11.22 VPN 方式接入内部网络过程

门户网站就是建立一个统一的内部网络资源入口,一切对内部网络资源的访问必须登录门户网站后才能进行,由门户网站完成对访问者的身份认证,并根据访问者的访问权限对访问过程实施控制。

11.3.1 系统结构

门户网站应用系统结构如图 11.23 所示,门户网站有两个接口,分别连接内部网络和外部网络,连接内部网络的接口分配内部网络本地 IP 地址,连接外部网络的接口分配全球 IP 地址。防火墙设置保证内部网络用户只能直接访问门户网站,不允许绕过门户网站直接访问内部网络服务器,外部网络终端也只能直接访问门户网站,只有通过门户网站才能访问到内部网络资源,门户网站作为应用层代理,在用户和服务器之间完成中继功能,如图 11.24 所示。

11.3.2 系统配置

1. 防火墙配置

防火墙配置要求只允许内部网络用户访问门户网站,只允许门户网站发起对服务器的访问过程,以此保证内部网络用户必须通过门户网站实现对服务器的访问。防火墙端

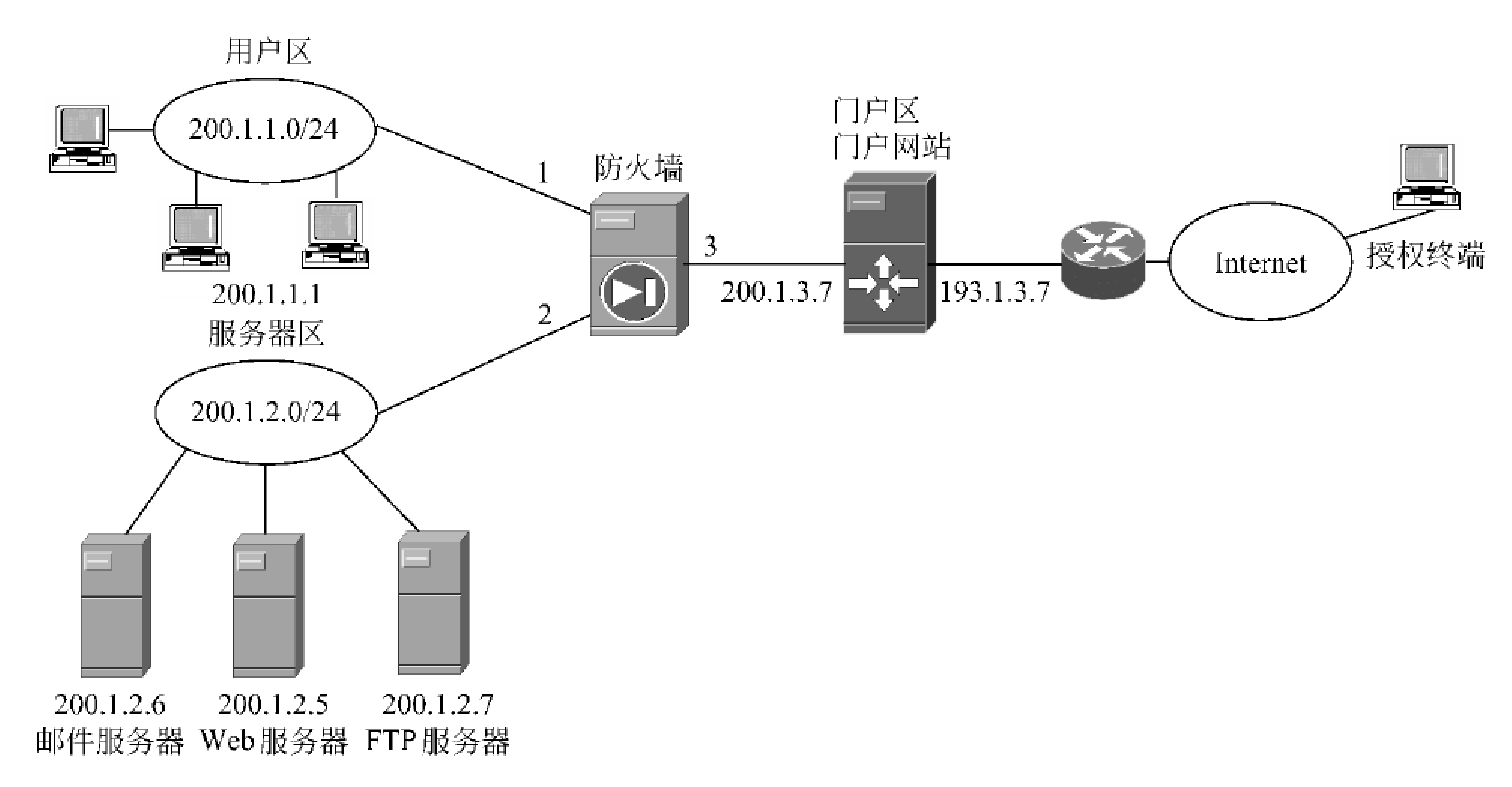


图 11.23　门户网站应用系统结构

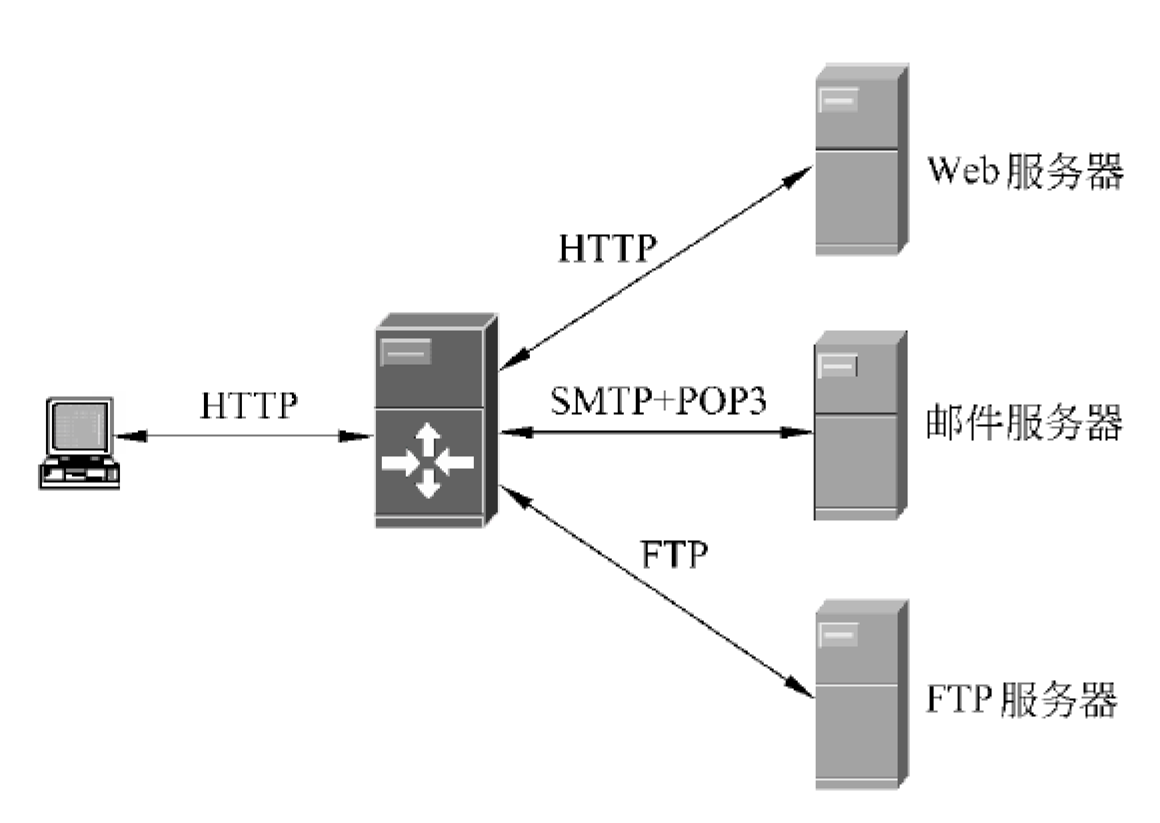


图 11.24　门户网站中继功能

口 1、2 和 3 分别绑定用户区、服务器区和门户区，配置以下用于控制区间信息传输过程的访问控制策略：

(1) 从用户区到门户区　源 IP 地址＝200.1.1.0/24　目的 IP 地址＝200.1.3.7/32　HTTP 服务；

(2) 从门户区到服务器区　源 IP 地址＝200.1.3.7/32　目的 IP 地址＝200.1.2.5/32　HTTP 服务；

(3) 从门户区到服务器区　源 IP 地址＝200.1.3.7/32　目的 IP 地址＝200.1.2.7/32　FTP 服务；

(4) 从门户区到服务器区　源 IP 地址＝200.1.3.7/32　目的 IP 地址＝200.1.2.6/32　SMTP＋POP3 服务。

2. 门户网站配置

内部网络用户可以采用 HTTP 访问门户网站，但为了安全，外部网络用户必须采用 HTTPS 访问门户网站，以此保证经过 Internet 传输的内部网络资源的保密性和完整性。为

此,将连接内部网络的接口的 IP 地址作为内部网络用户用 HTTP 访问门户网站的 IP 地址,用 HTTP 的默认端口 80 作为侦听端口,将连接外部网络的接口的 IP 地址作为外部网络用户用 HTTPS 访问门户网站的 IP 地址,用 HTTPS 的默认端口 443 作为侦听端口。

URL:200.1.3.7:80,HTTP

URL:193.1.3.7:443 HTTPS

配置每一个用户的访问权限,同一用户随着访问时的位置(内部网络或外部网络)不同,其访问权限也不同,表 11.4 是为门户网站配置的用户访问权限。

表 11.4　用户访问权限

用户名	认证机制	访问方式	资源名称
用户 *A*	HTTPS 证书+数字签名	FTP(用户 *A*,PASSA)	200.1.2.7/ABC/ *
		HTTP	200.1.2.5/SALE/ *
		SMTP+POP3(用户 *A*,PASSA)	UserA@200.1.2.6
用户 *A*	HTTP 口令:PASSA	FTP(用户 *A*,PASSA) (SUPP,SUPPA)	200.1.2.7/ABC/ * 200.1.2.7/TECH/ *
		HTTP	200.1.2.5/SALE/ * 200.1.2.5/SUPP/ *
		SMTP+POP3(用户 *A*,PASSA) (SUPP,SUPPA)	UserA@200.1.2.6 SUPP@200.1.2.6
⋮	⋮	⋮	⋮

表 11.4 表明用户 *A* 如果在外部网络通过 HTTPS 登录,只允许访问邮件服务器中自己的信箱(UserA@200.1.2.6),FTP 服务器中一般目录下的文件(/ABC/ *)和 Web 服务器中有关对外销售宣传的网页内容(/SALE/ *),并给出访问应用服务器时需要给出的口令和用户名,当然,这些口令和用户名也可以在访问过程中由用户通过门户网站推送的网页直接输入。如果从内部网络登录,需要确认用户口令 PASSA(当然,实际实现中,以更安全的方式来存放口令),允许访问的内部网络资源更多,如 FTP 服务器中有关企业产品的技术资料(/TECH/ *),Web 服务器中和技术支持有关的网页(/SUPP/ *)和邮件服务器中客户请求技术支持的信箱(SUPP@200.1.2.6)。对所有允许访问内部网络资源的用户配置访问权限后,门户网站将严格依据每一个用户的访问权限对访问过程实施控制。在实际应用过程中,每一个用户还可以绑定一个对内容进行过滤处理的组件,门户网站向用户转发服务器响应消息前,可用绑定的组件对响应消息内容进行过滤处理。

11.3.3　实现机制

下面以用户 *A* 通过外部网络下载 FTP 服务器中文件 200.1.2.7/ABC/DEC.DOC 为例,讨论门户网站实施访问控制的机制。

1. 获取证书链

在开始访问过程前,门户网站和用户 *A* 必须获取用于证明自己身份的证书链,双方拥有的证书链必须能够认证对方用于证明自己身份的证书。

2. 登录门户网站

用户 *A* 在浏览器地址栏中输入：HTTPS:// 193.1.3.7。

用户 *A* 和门户网站进行图 11.25 所示的 TLS 连接建立过程。在建立 TLS 连接后，门户网站向用户 *A* 推送网页，该网页用于用户 *A* 输入需要访问的资源名称及对应的访问方式。

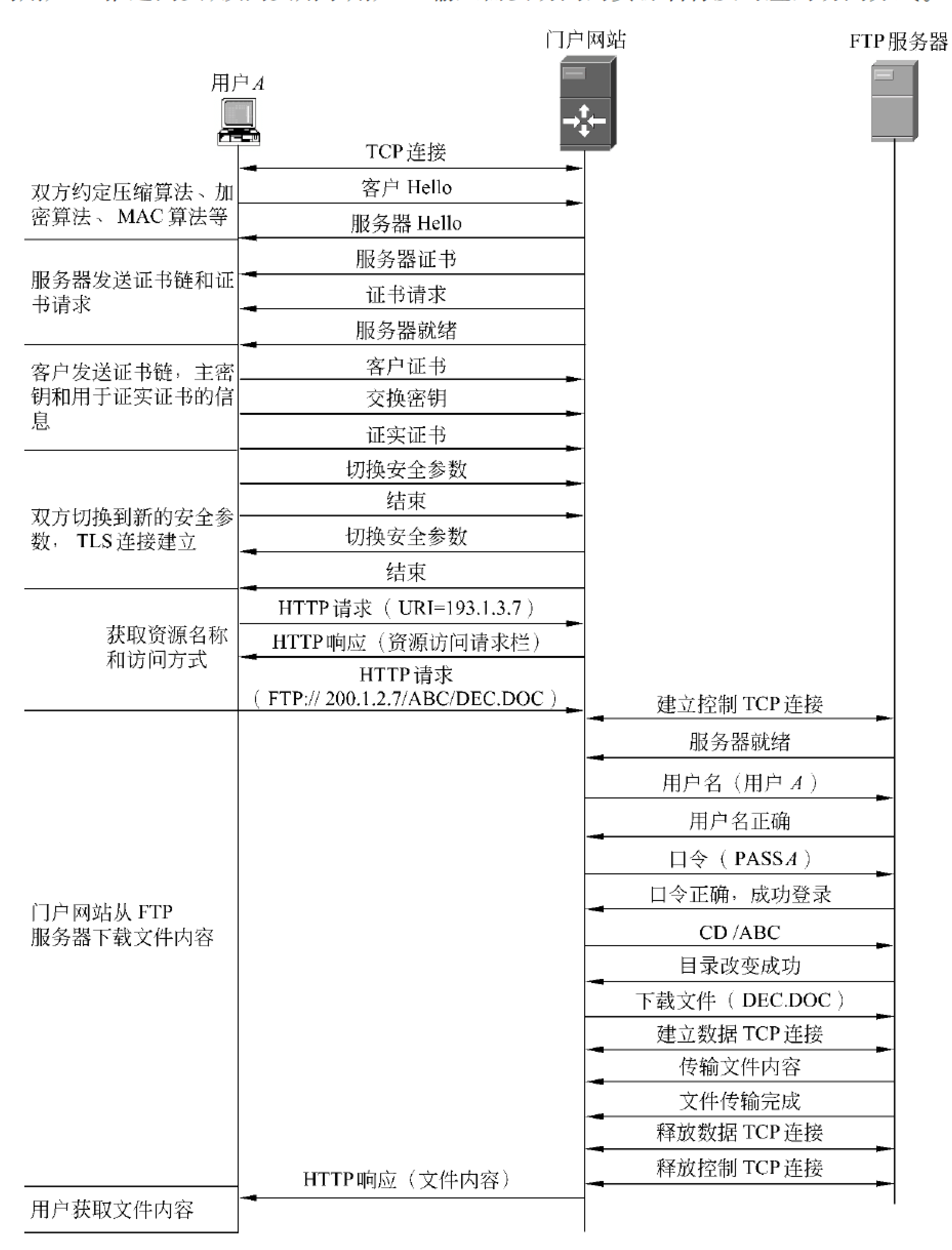


图 11.25　用户通过门户网站访问网络资源过程

3. 访问资源

用户 *A* 在门户网站推送的网页中输入访问方式和资源名称：

FTP://200.1.2.7/ABC/DEC.DOC

当然，门户网站和用户 A 交换的信息都封装成 TLS 记录协议报文，并以建立 TLS 连接时产生的密钥进行加密。

门户网站对用户 A 输入的访问方式和资源名称进行检测，确定是否符合为其分配的访问权限，在访问权限检测通过后，进行图 11.25 所示的 FTP 服务器访问过程，在获得文件内容后，将其封装成 HTTP 响应消息格式，并经过 TLS 连接传输给用户 A。

习 题

11.1 给出用 IPSec 实现 Web 安全的思路，并比较 IPSec、HTTPS 和 SET 的优缺点。

11.2 HTTPS 实现 Web 安全的基本思路是什么？和 SET 有什么本质区别？

11.3 在 HTTPS Web 安全机制中，TLS 记录协议的功能是什么？

11.4 用户通过网上银行实现电子转账时，银行可以用于证明该次电子转账确实由用户本人完成的凭证是什么？用户通过 SET 实现电子转账时，银行可以用于证明该次电子转账确实由用户本人申请的凭证是什么，它们之间有什么区别？

11.5 在一个使用 SET 的网络购物过程后，用户、银行和商家各自具有哪些证明该次交易正常完成的凭证？这些凭证用于解决什么纠纷？

11.6 PGP 提供哪些基本服务？

11.7 PGP 为什么在压缩操作前产生数字签名？

11.8 S/MIME 实现邮件安全传输的基本思路是什么？它和 PGP 有什么异同？

11.9 门户网站的作用是什么？

11.10 门户网站认证用户身份的机制有哪些？精确控制每一个用户允许访问的网络资源的机制有哪些？

11.11 网络结构如图 11.26 所示，要求对终端访问服务器（Web 服务器和 FTP 服务器）过程实施统一控制，访问对象能够精确到文件，在网络中增加必需的设备，并给出对实施统一访问控制有关的配置信息。

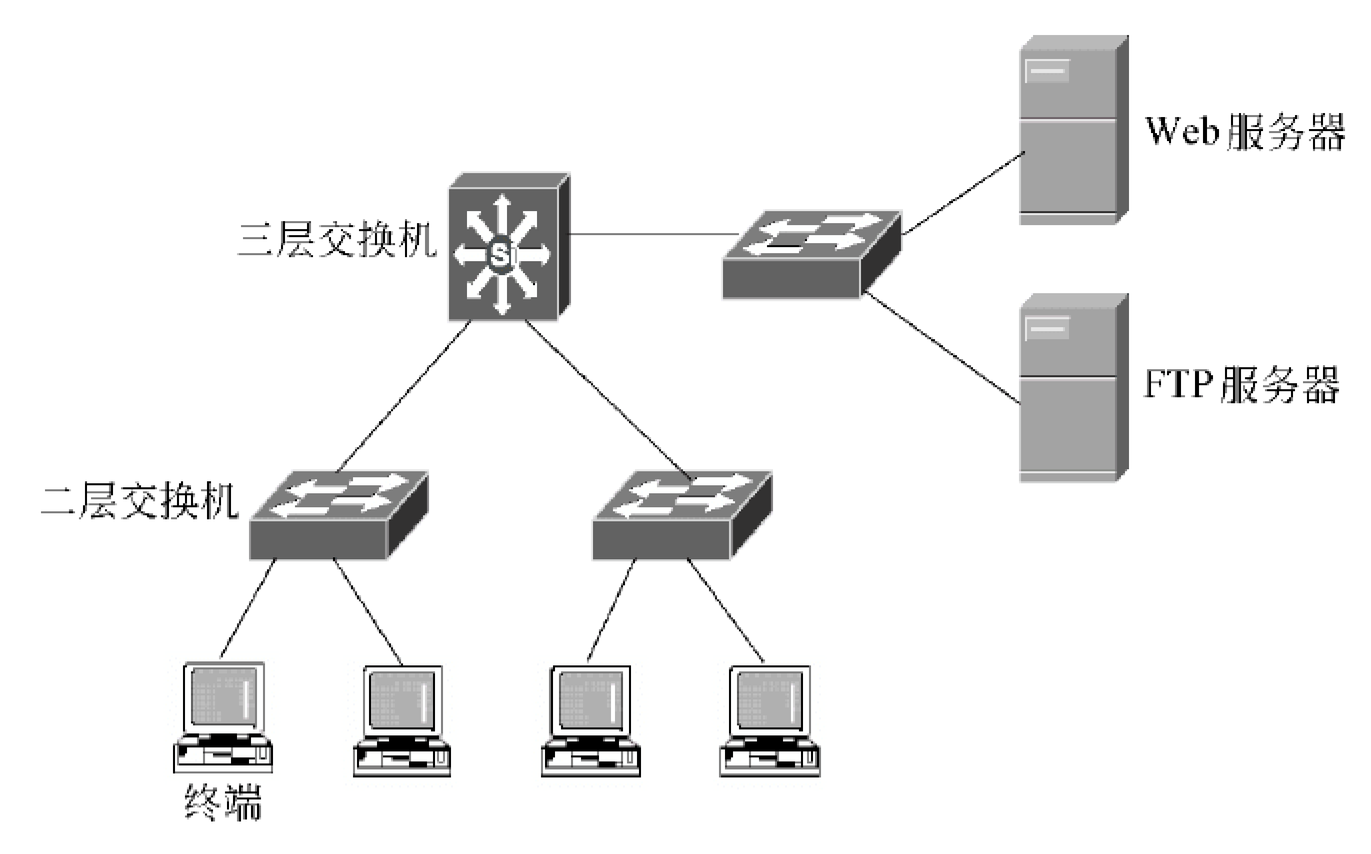


图 11.26 题 11.11 图

附录 A 英文缩写词

ADDENDUM

ADSL(Asymmetric Digital Subscriber Line)非对称数字用户线(1.4.2)
AES(Advanced Encryption Standard)高级加密标准(3.1.1)
AH(Authentication Header)认证首部(3.5.2)
AP(Access Point)接入点(1.3.2)
ATM(Asynchronous Transfer Mode)异步传输模式(6.1.1)
AVP(Attribute Value Pair)属性值对(6.3.2)
BSS(Basic Service Sets)基本服务集(1.3.2)
CA(Certification Authority)认证中心(3.3.2)
CBC(Cipher-Block Chaining)加密分组链接(3.1.1)
CCMP(CTR with CBC-MAC Protocol)(5.4.1)
CE(Customers' Edge router)用户边缘路由器(6.1.1)
CHAP(Challenge Handshake Authentication Protocol)挑战握手认证协议(3.4.3)
CRC(Cyclic Redundancy Check)循环冗余检验(5.2.2)
DES(Data Encryption Standard)数据加密标准(3.1.1)
DHCP(Dynamic Host Configuration Protocol)动态主机配置协议(4.1.2)
DMZ(Demilitarized Zone)非军事区(1.3.3)
DNS(Domain Name System)域名系统(2.3.3)
DOS(Denial Of Service)拒绝服务(2.1.3)
DS(Dual Signature)双重签名(11.1.4)
EAP(Extensible Authentication Protocol)扩展认证协议(3.4.3)
ESP(Encapsulating Security Payload)封装安全净荷(3.5.3)
FTP(File Transfer Protocol)文件传输协议(7.2.2)
GTK(Group Temporal Key)临时广播密钥(5.4.3)
HIPS(Host Intrusion Prevention System)主机入侵防御系统(8.1.1)
HMAC(Hashed Message Authentication Codes)散列消息认证码(3.2.4)
HTTP(Hyper Text Transfer Protocol)超文本传输协议(1.4.2)
HTTPS(HTTP over TLS)(11.1.3)
ICV(Integrity Check Value)完整性检验值(1.2.3)
IIS(Internet Information Service)Internet 信息服务(2.1.1)
IP(Internet Protocol)网际协议(1.1.1)

IPS (Intrusion Prevention System)入侵防御系统(8.1)
IPSec(IP Security,IP 安全协议)(3.5)
ISAKMP (Internet 安全关联和密钥管理协议 Internet Security Association and Key Management Protocol)(3.5.4)
ISM(Industrial,Scientific,and Medical)工业、科学和医疗频段
ISP(Internet Service Provider)Internet 服务提供者(3.4.4)
KCK(EAPOL-Key Confirmation Key)证实密钥(5.4.3)
KDC(Key Distribution Center)密钥分配中心(3.1.1)
KEK(EAPOL-Key Encryption Key)加密密钥(5.4.3)
L2TP(Layer Two Tunneling Protocol)第 2 层隧道协议(6.1.1)
LAC(Access Concentrator)L2TP 接入集中器(6.1.1)
LAN(Local Area Network)局域网(4.2.1)
LNS(L2TP Network Server)L2TP 网络服务器(6.1.1)
LSP(Label Switched Path)标签交换路径(4.3.3)
MAC(Medium Access Control)媒体接入控制(1.3.2)
MAC(Message Authentication Code)消息认证码(3.4.2)
MD(Message Digest)报文摘要(1.3.1)
MD5(Message Digest ,Version 5)报文摘要第 5 版(3.2.1)
MIB(Management Information Base)管理信息库(9.1.1)
MIC(Message Integrity Code)消息完整性编码(1.2.3)
MIME(Multipurpose Internet Mail Extension)通用 Internet 邮件扩充(11.2.2)
MPLS(MultiProtocol Label Switching)多协议标签交换(6.1.1)
MSRPC(Microsoft Remote Procedure Call)微软远程过程调用(2.1.1)
MTU(Maximum Transfer Unit)最大传送单元(3.5.1)
NAS(Network Access Server)网络接入服务器(3.4.4)
NAT(Network Address Translation)网络地址转换(4.5)
NBNS(NetBIOS Names Service)NetBIOS 名字解析服务(2.1.1)
NIPS(Network Intrusion Prevention System)网络入侵防御系统(8.1.1)
NMS(Network Management Station)网络管理工作站(9.1.1)
OI(Order Information)订货信息(11.1.4)
PAE(Port Access Entity)端口接入实体(3.4.3)
PAT(Port Address Translation)端口地址转换(4.5.1)
PE(Service Provider's Edge router)提供者边缘路由器(6.1.1)
PGP(Pretty Good Privacy)一种安全传输电子邮件的协议(11.2.1)
PKI(Public Key Infrastructure)公开密钥设施(3.3.2)
PI(Payment Information)支付信息(11.1.4)
PMK(Pairwise Master Key)成对主密钥(5.4.2)
POP3(Post Office Protocol 3)邮局协议第 3 版(7.2.2)
PTK(Pairwise Transient Key)成对过渡密钥(5.4.3)
PPP(Point-to-Point Protocol)点对点协议(3.4.3)
PPPoE(PPP over Ethernet)基于以太网的 PPP(3.4.3)
PSTN(Public Switched Telephone Network)公共交换电话网(2.2.1)

RADIUS(Remote Authentication Dial In User Service)远程认证拨入用户服务(3.4.4)
RSA(Rivest-Shamir-Adleman)一种公开密钥加密算法(3.1.2)
SA(Security Association)安全关联(3.5.1)
SET(Secure Electronic Transaction)安全电子交易(11.1.4)
SDH(Synchronous Digital Hierarchy)同步数字体系(6.1)
SHA-1(Secure Hash Algorithm 1)安全散列算法第 1 版(3.2.3)
SPD(Security Policy Database)安全策略数据库(3.5.1)
SPI(Security Parameters Index)安全参数索引(3.5.1)
SMB(Server Message Block)服务器消息块(2.1.1)
S/MIME(Secure/Multipurpose Internet Mail Extension)增加安全功能的通用 Internet 邮件扩充(11.2.2)
SMTP(Simple Mail Transfer Protocol)简单邮件传输协议(7.2.2)
SNMP(Simple Network Management Protocol)简单网络管理协议(9.1.1)
SSID(Service Set IDentifier)服务集标识符(2.3.2)
STP(Spanning Tree Protocol)生成树协议(4.6.3)
TCP(Transmission Control Protocol)传输控制协议(1.1.1)
TK(Temporal Key)临时密钥(5.4.1)
TKIP(Temporal Key Integrity Protocol)临时密钥完整性协议(5.4.1)
TLS(Transport Layer Security)运输层安全(3.4.2)
TSC(TKIP Sequence Counter)序号计数器(5.4.1)
UAC(Unified Access Control)统一访问控制(7.4)
VC(Virtual Circuit)虚电路(6.1.1)
VFI(Virtual Forwarding Instance)虚拟转发实体(6.4.1)
VLAN(Virtual LAN)虚拟局域网(4.3.1)
VPLS(Virtual Private LAN Service)虚拟专用局域网服务(6.1.1)
VPN(Virtual Private Network)虚拟专用网(4.3.3)
VR(Virtual Router)虚拟路由器(4.3.2)
WEP(Wired Equivalent Privacy)等同有线安全(2.1.1)
WLAN(Wireless LAN)无线局域网(5.1)

参 考 文 献

1 William Stallings. NETWORK SECURITY ESSENTIALS APPLICATIONS AND STANDARDS Second Edition. 北京：清华大学出版社，2005.

2 Stuart McClure，Joel Scambray，George Kurtz 著. 黑客大曝光(第 5 版). 王吉军，张玉亭，周维续译. 北京：清华大学出版社，2006.

3 Andrew S. Tanenbaum Computer Networks Fourth Edition. 北京：清华大学出版社，2004.

4 谢希仁. 计算机网络(第 4 版). 北京：电子工业出版社，2003.

5 沈鑫剡. 计算机网络. 北京：清华大学出版社，2008.

6 沈鑫剡，俞海英，伍红兵，胡勇强. 计算机网络技术及应用. 北京：清华大学出版社，2007.

7 沈鑫剡等. 多媒体传输网络与 VOIP 系统设计. 北京：人民邮电出版社，2005.

8 沈鑫剡等. IP 交换网原理、技术及实现. 北京：人民邮电出版社，2003.

9 沈鑫剡. 广域网原理、技术及实现. 北京：人民邮电出版社，2000.

10 沈鑫剡. 交换式以太网原理、技术及实现. 北京：人民邮电出版社，1999.

11 James Trulove 著. 局域网布线. 沈鑫剡译. 北京：人民邮电出版社，2002.

12 http://www. ietf. org/

13 http://standards. ieee. org/

14 http://www. cisco. com/

15 http://www. 3com. com/

16 http://www. juiper. net/

普通高校本科计算机专业特色教材精选

计算机硬件

MCS 296 单片机及其应用系统设计　刘复华　ISBN 978-7-302-08224-8
基于 S3C44B0X 嵌入式 μcLinux 系统原理及应用　李岩　ISBN 978-7-302-09725-9
现代数字电路与逻辑设计　高广任　ISBN 978-7-302-11317-1
现代数字电路与逻辑设计题解及教学参考　高广任　ISBN 978-7-302-11708-7

计算机原理

汇编语言与接口技术(第 2 版)　王让定　ISBN 978-7-302-15990-2
汇编语言与接口技术习题汇编及精解　朱莹　ISBN 978-7-302-15991-9
基于 Quartus Ⅱ 的计算机核心设计　姜咏江　ISBN 978-7-302-14448-9
计算机操作系统(第 2 版)　彭民德　ISBN 978-7-302-15834-9
计算机维护与诊断实用教程　谭祖烈　ISBN 978-7-302-11163-4
计算机系统的体系结构　李学干　ISBN 978-7-302-11362-1
计算机选配与维修技术　闵东　ISBN 978-7-302-08107-4
计算机原理教程　姜咏江　ISBN 978-7-302-12314-9
计算机原理教程实验指导　姜咏江　ISBN 978-7-302-15937-7
计算机原理教程习题解答与教学参考　姜咏江　ISBN 978-7-302-13478-7
计算机综合实践指导　宋雨　ISBN 978-7-302-07859-3
实用 UNIX 教程　蒋砚军　ISBN 978-7-302-09825-6
微型计算机系统与接口　李继灿　ISBN 978-7-302-10282-3
微型计算机系统与接口教学指导书及习题详解　李继灿　ISBN 978-7-302-10559-6
微型计算机组织与接口技术　李保江　ISBN 978-7-302-10425-4
现代微型计算机与接口教程(第 2 版)　杨文显　ISBN 978-7-302-15492-1
智能技术　曹承志　ISBN 978-7-302-09412-8

软件工程

软件工程导论(第 4 版)　张海藩　ISBN 978-7-302-07321-5
软件工程导论学习辅导　张海藩　ISBN 978-7-302-09213-1
软件工程与软件开发工具　张虹　ISBN 978-7-302-09290-2

数据库

数据库原理及设计(第 2 版)　陶宏才　ISBN 978-7-302-15160-9

数理基础

离散数学　邓辉文　ISBN 978-7-302-13712-5
离散数学习题解答　邓辉文　ISBN 978-7-302-13711-2

算法与程序设计

C/C++ 语言程序设计　孟军　ISBN 978-7-302-09062-5
C++ 程序设计解析　朱金付　ISBN 978-7-302-16188-2
C 语言程序设计　马靖善　ISBN 978-7-302-11597-7
C 语言程序设计(C99 版)　陈良银　ISBN 978-7-302-13819-8
Java 语言程序设计　吕凤翥　ISBN 978-7-302-11145-0
Java 语言程序设计题解与上机指导　吕凤翥　ISBN 978-7-302-14122-8
MFC Windows 应用程序设计(第 2 版)　任哲　ISBN 978-7-302-15549-2
MFC Windows 应用程序设计习题解答及上机实验(第 2 版)　任哲　ISBN 978-7-302-15737-3

Visual Basic. NET 程序设计　刘炳文	ISBN 978-7-302-16372-5
Visual Basic. NET 程序设计题解与上机实验　刘炳文	ISBN 978-7-302-16870-6
Windows 程序设计教程　杨祥金	ISBN 978-7-302-14340-6
编译设计与开发技术　斯传根	ISBN 978-7-302-07497-7
汇编语言程序设计　朱玉龙	ISBN 978-7-302-06811-2
数据结构(C ++ 版)　王红梅	ISBN 978-7-302-11258-7
数据结构(C ++ 版)教师用书　王红梅	ISBN 978-7-302-15128-9
数据结构(C ++ 版)学习辅导与实验指导　王红梅	ISBN 978-7-302-11502-1
数据结构(C 语言版)　秦玉平	ISBN 978-7-302-11598-4
算法设计与分析　王红梅	ISBN 978-7-302-12942-4

图形图像与多媒体技术

多媒体技术实用教程(第 2 版)　贺雪晨	ISBN 978-7-302-16854-6
多媒体技术实用教程(第 2 版)实验指导　贺雪晨	ISBN 978-7-302-16907-9

网络与通信

计算机网络　胡金初	ISBN 978-7-302-07906-4
计算机网络实用教程　王利	ISBN 978-7-302-14712-1
数据通信与网络技术　周昕	ISBN 978-7-302-07940-8
网络工程技术与实验教程　张新有	ISBN 978-7-302-11086-6
计算机网络管理技术　杨云江	ISBN 978-7-302-11567-0
TCP/IP 网络与协议　兰少华	ISBN 978-7-302-11840-4

读者意见反馈

亲爱的读者：

感谢您一直以来对清华版计算机教材的支持和爱护。为了今后为您提供更优秀的教材，请您抽出宝贵的时间来填写下面的意见反馈表，以便我们更好地对本教材做进一步改进。同时如果您在使用本教材的过程中遇到了什么问题，或者有什么好的建议，也请您来信告诉我们。

地址：北京市海淀区双清路学研大厦 A 座 602 室　计算机与信息分社营销室 收
邮编：100084　　电子邮件：jsjjc@tup.tsinghua.edu.cn
电话：010-62770175-4608/4409　　邮购电话：010-62786544

教材名称：计算机网络安全
ISBN：978-7-302-20397-1
个人资料
姓名：________ 年龄：______ 所在院校/专业：____________
文化程度：________ 通信地址：____________________
联系电话：________ 电子信箱：____________________
您使用本书是作为：□指定教材 □选用教材 □辅导教材 □自学教材
您对本书封面设计的满意度：
□很满意 □满意 □一般 □不满意　改进建议____________________
您对本书印刷质量的满意度：
□很满意 □满意 □一般 □不满意　改进建议____________________
您对本书的总体满意度：
从语言质量角度看 □很满意 □满意 □一般 □不满意
从科技含量角度看 □很满意 □满意 □一般 □不满意
本书最令您满意的是：
□指导明确 □内容充实 □讲解详尽 □实例丰富
您认为本书在哪些地方应进行修改？（可附页）
____
____
您希望本书在哪些方面进行改进？（可附页）
____
____

电子教案支持

敬爱的教师：

为了配合本课程的教学需要，本教材配有配套的电子教案（素材），有需求的教师可以与我们联系，我们将向使用本教材进行教学的教师免费赠送电子教案（素材），希望有助于教学活动的开展。相关信息请拨打电话 010-62776969 或发送电子邮件至 jsjjc@tup.tsinghua.edu.cn 咨询，也可以到清华大学出版社主页（http://www.tup.com.cn 或 http://www.tup.tsinghua.edu.cn）上查询。